NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PROTECTING NEW YORK'S INFRASTRUCTURE: IMPROVING OVERALL SAFETY AND SECURITY THROUGH NEW PARTNERSHIPS AND CONCENTRATION ON PLANNING, ENGINEERING AND DESIGN

by

John M. McNamara

December 2013

Thesis Advisor: Lauren Fernandez
Second Reader: Brian Nussbaum

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE PROTECTING NEW YORK'S INFRASTRUCTURE: IMPROVING OVERALL SAFETY AND SECURITY THROUGH NEW PARTNERSHIPS AND CONCENTRATION ON PLANNING, ENGINEERING AND DESIGN			**5. FUNDING NUMBERS**
6. AUTHOR(S) John M. McNamara			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The infrastructure that supports New York State and its citizens is constantly faced with threats that test its resilience. These threats range from those brought upon by nature, and man-made threats, such as those from terrorists. Understanding these threats are persistent, and the challenge of infrastructure protection is complex. Stakeholders must consider methods to mitigate risk. This paper seeks to answer two questions, both of which strive to decrease risk over the long term for the state's citizens. First, what are the benefits and challenges of the state placing a greater focus on the planning, engineering, and design phase for new or significantly reconstructed infrastructure? Second, how could a new partnership model at the state level be designed to support infrastructure protection activities during this phase? To accomplish these two outcomes, three approaches focused on planning and design within the public and private sector are analyzed and compared. This paper expands upon the partnership incentives utilized to reach desired outcomes in such infrastructure programs. Finally, this research concludes that the state should do more to improve safety and security during the planning, engineering and design phase and recommends two parallel paths forward for implementation at the state level.

14. SUBJECT TERMS Infrastructure, Infrastructure Protection, Planning, Engineering and Design, Partnership Model, Resilience			**15. NUMBER OF PAGES** 89
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

PROTECTING NEW YORK'S INFRASTRUCTURE: IMPROVING OVERALL SAFETY AND SECURITY THROUGH NEW PARTNERSHIPS AND CONCENTRATION ON PLANNING, ENGINEERING AND DESIGN

John M. McNamara
Division of Homeland Security and Emergency Services,
New York State, Office of Counter Terrorism, Albany, NY
B.S., Niagara University, 2002

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2013**

Author: John M. McNamara

Approved by: Lauren Fernandez, DSc
Thesis Advisor

Brian Nussbaum, PhD
Second Reader

Mohammed Hafez
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The infrastructure that supports New York State and its citizens is constantly faced with threats that test its resilience. These threats range from those brought upon by nature, and man-made threats, such as those from terrorists. Understanding these threats are persistent, and the challenge of infrastructure protection is complex. Stakeholders must consider methods to mitigate risk. This paper seeks to answer two questions, both of which strive to decrease risk over the long term for the state's citizens. First, what are the benefits and challenges of the state placing a greater focus on the planning, engineering, and design phase for new or significantly reconstructed infrastructure? Second, how could a new partnership model at the state level be designed to support infrastructure protection activities during this phase? To accomplish these two outcomes, three approaches focused on planning and design within the public and private sector are analyzed and compared. This paper expands upon the partnership incentives utilized to reach desired outcomes in such infrastructure programs. Finally, this research concludes that the state should do more to improve safety and security during the planning, engineering and design phase and recommends two parallel paths forward for implementation at the state level.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CABE	Commission for Architecture and the Built Environment
CBAT	Computer Based Assessment Tool
CFATS	Chemical Facilities Anti-Terrorism Standards
CPNI	Centre for the Protection of National Infrastructure
CPTED	Crime Prevention Through Environmental Design
DBT	Design Basis Threat
DHS	Department of Homeland Security
DHSES	Division of Homeland Security and Emergency Services
DOB	Department of Budget
EO	Executive Order
EVAP	Enhanced Visual Assessment Program
FEMA	Federal Emergency Management Agency
FOUO	For Official Use Only
GSA	General Services Administration
HMGP	Hazard Mitigation Grant Program
HSGP	Homeland Security Grant Program
IAEA	International Atomic Energy Agency
IAV	Initial Asset Visit
IPD	Integrated Project Delivery
ISC	Interagency Security Committee
IST	Infrastructure Survey Tool
LEED	Leadership in Energy & Environmental Design
MTA	Metropolitan Transit Authority
NIPP	National Infrastructure Protection Plan
NRR	National Risk Register
NYC	New York City
NYPD	New York City Police Department
NYS	New York State
OCT	Office of Counter Terrorism
OCT-CI	Critical Infrastructure Protection Unit
OGS	Office of General Services

SAA	State Administrative Agency
SAV	Site Assistance Visits
SIDOS	Security in Design of Stations
SHSP	State Homeland Security Program
UK	United Kingdom
U.S.	United States

EXECUTIVE SUMMARY

Infrastructure protection is a simple phrase that masks the complexity of its actual nature. Persistent and dynamic threats place these assets, and the communities that rely upon them, at risk of losing their services, which can cause collateral damage, and in the worst-case scenario, potential loss of life. Once an infrastructure project has been funded, the planning, engineering, and design phase of a project offers an invaluable opportunity to evaluate potential threats and hazards. Next, mitigation options can be explored to protect the asset and society throughout its operational life, and be implemented at a lower cost to the owner/operator than retrofitting once built.

Many issues contribute to the challenges associated with ensuring appropriate infrastructure protection. Some issues, such as the aging infrastructure dilemma, are fairly straightforward. Others created by human nature, such as the psychology of reacting to an event that then skews mitigation efforts too far towards one extreme or another, can be extremely complex. Aggregated together with the increasing use of public and private partnerships and it becomes clear more should be done to improve upon current efforts.

To understand what New York State (NYS) should do, this thesis applied a pragmatic qualitative approach using case studies to assess variations in assessment and cooperation frameworks. Recognizing the existence of the problem area, the literature review was leveraged to determine what has been accomplished thus far within the infrastructure protection field in both the public and private realm and focuses on planning, engineering, and design. Additionally, this review provided an informed understanding of the complexity of the planning and design field. With this background, the research questions could begin to be addressed.

- What are the benefits and challenges of NYS placing a greater focus on the planning, engineering, and design phase for new or majorly reconstructed infrastructure?
- How could a new partnership model at the state level be designed to support infrastructure protection activities during this phase?

Three different approaches were analyzed representing the infrastructure spectrum: simple government, complex government, and the private sector. This analysis was then expanded to understand in more detail the varieties of incentives for participation and their general effectiveness. Two recommendations and suggested paths forward were then developed. These recommendations would impact state-owned and leased buildings and state-financed infrastructure.

As it pertains to state-owned and leased buildings, this research recommends that security standards be promulgated that would apply to new or majorly reconstructed buildings. To that end, it is recommended that the Division of Homeland Security and Emergency Services (DHSES) partner with the Office of General Services; Security and Emergency Management Unit, and its existing membership. Leveraging smart practices developed by the General Services Administration (GSA), the newly formed group could develop standards appropriate for the state, and begin an incremental process of improving safety and security at its infrastructure.

Affecting change for state-financed infrastructure is a more complex and challenging goal, yet one this research finds important on which to act. It is recommended that when state funds are provided to assist with creating a new infrastructure asset or major reconstruction project, the bidding and procurement process require the development and inclusion of a design based threat and subsequent development of security performance specifications. This approach would influence change over a broader range of assets and ensure tax dollars are spent with the citizen's safety and security as a priority.

This recommendation would assign the Office of Counter Terrorism under DHSES supervision as the lead for this project. Current efforts underway within the Rebuild NY program could be leveraged to establish a pilot project in which these concepts could be tested and evaluated. After review, if deemed successful, this concept could be implemented to the larger community with an identified minimum project threshold based on cost (monetary amount established to exclude minor projects), scope, criticality, or related characteristics.

These recommended changes would be challenging to implement. Challenges, such as obtaining executive support, personnel constraints, and competing priorities that require consideration were taken into account in the development of these recommendations. In the end, this research concluded that those obstacles are not significant enough to prevent forward progress in this area.

Overall recommended change of focus for NYS in the planning, engineering, and design environment will greatly assist the state's infrastructure over the long term. Starting this process by first improving state-owned and leased buildings will demonstrate to the community that NYS takes this subject matter seriously. Additionally, requiring security to be a focus for assets receiving state funds will demonstrate the same priorities to contractors and the community.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my wife, Liz, and children, Dermot and Bridget, for their incredible support and patience while I dove back into the academic world. Accomplishing this goal would also not have been possible without the steady support of my parents, Dave and Kathy. I would also like to thank the Division of Homeland Security and Emergency Services for providing me the opportunity to attend the Naval Postgraduate School.

To my friends from Cohort 1203/1204, I have learned much from you over our time together and look forward to leveraging the new network we have built. Finally, to my thesis support team, Lauren Fernandez and Brian Nussbaum, you have guided an infantryman through this academic effort with amazing skill, and for that, I am truly grateful.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Infrastructure protection[1] is a simple phrase that masks the complexity of its actual nature. Persistent and dynamic threats place these assets, and the communities that rely upon them, at risk of losing their services, cause collateral damage, and in the worst-case scenario, potential loss of life. Once an infrastructure project has been funded, the planning and design phase of a project offers an invaluable opportunity to evaluate potential threats and hazards. Next, mitigation options can be explored to protect the asset and society throughout its operational life, and implemented at a lower cost to the owners/operators than retrofitting once built. This thesis explores how safety and security can effectively be incorporated during the planning and design phase.

A. DEFINING THE PROBLEM

In New York State (NYS), the most recent disaster that dramatically affected the community was Hurricane Sandy. As with most events that create a great deal of devastation, public and private stakeholders have placed a tremendous focus since the incident on understanding what has occurred, identifying lessons learned, and establishing plans to mitigate future risk. Although the scale and scope of the review of Hurricane Sandy is massive and wide ranging, significant time and effort was spent focusing on the state's infrastructure. Governor Andrew M. Cuomo formed three commissions charged with reviewing and providing recommendations to improve the state's ability to endure future threats and hazards: the NYS 2100 Commission, the NYS Respond Commission, and the NYS Ready Commission.[2] Each commission incorporated and considered state infrastructure within its review. Similar efforts and reviews have occurred at local jurisdictional levels as well; the New York City (NYC) Hurricane

[1] Infrastructure protection is the efforts taken by all relevant stakeholders to ensure the environment that the asset could affect is safe and secure.

[2] Governor's Press Office, *Governor Cuomo Announces Commissions to Improve New York State's Emergency Preparedness and Response Capabilities, and Strengthen the State's Infrastructure to Withstand Natural Disasters* (New York State: November 28, 2012).

Sandy After Action Report highlighted and recommended major improvements to essential community services and business infrastructure recovery efforts.[3]

The *NYS 2100 Commission Report* concluded, "It is incumbent upon the State to plan, finance, fund and support a range of infrastructure solutions in order to ensure that our economy and communities are resilient in the 21st century."[4] Through the Federal Emergency Management Agency (FEMA) Hazard Mitigation Grant Program (HMGP), the state is managing a grant program available to local governments to address areas, such as the following.[5]

- Reducing the risk of flood damage at government, non-profit and private sector assets
- Mitigating vulnerabilities on transportation, communications, and energy assets
- Implementing eligible mitigation recommendations identified within the NYS Commission reports

As these necessary solutions become real projects, infrastructure stakeholders will be faced with the challenges of the planning, engineering, and design phase leading to a successful project completion. The NYS government will be providing financial resources in support of many of these projects; what responsibilities does it carry to ensure the goal of resilience is achieved? How can it best live up to these responsibilities?

For the purpose of this thesis, NYS infrastructure resilience will be addressed by exploring how the government can be more proactive than reactive with regards to improving infrastructure's ability to withstand and adapt to shocks and disasters, or to be brought back on line quickly following such events. Winston Churchill once said, "Never

[3] Linda Gibbs and Caswell Holloway, *Hurricane Sandy After Action: Report and Recommendations to Major Michael R. Bloomberg*, New York City, NY, 2013.

[4] Kevin E. McCarthy et al., *Recommendations on Improving Infrastructure Resilience Post-Sandy* (Hartford, CT: Connecticut General Assembly, Office of Legislative Research, 2013).

[5] New York State Office of Emergency Management, "Hazard Mitigation Grant Program," n.d., http://stormrecovery.ny.gov/content/hazard-mitigation-grant-program-hmgp-0.

let a good crisis go to waste."[6] NYS is leveraging this concept as federal and state funds are earmarked for addressing solutions identified by reports, such as the *NYS 2100 Commission Report*.

While undergoing the effort of creating a more resilient 21st century through improving NYS infrastructure, it is in the state's best interest to ensure it does not become too narrowly focused on the threat of Mother Nature. It is natural to prioritize the risk that is most fresh in people's minds; however, excluding other relevant threats from consideration during the mitigation process may create missed opportunities. With the continuing demonstrated intent of terrorists to attack this nation's homeland, it is critical for policies and programs to include the consideration of man-made threats, as well as natural hazards. Foiled attempts to attack the Empire State, such as those by Faisal Shahzad, Najibullah Zazi, and Jose Pimental, make this issue even more relevant for NYS. It is important to remember the lessons learned from 9/11 and ensure failure of imagination does not impact the community once again.

At certain moments in history, multiple problems and opportunities collide, which dramatically increases the importance of decisions to be made. Within a relatively short timeframe, NYS has experienced major man-made and natural disasters that have strained the governmental system.[7] Citizens expect government to ensure the services and support that infrastructure provides them are reliable and protected. To that end, the government can utilize many approaches and methods to meet or manage this expectation. This nation's infrastructure can be protected in many ways; it is a government's challenge to determine what is most effective, efficient, and appropriate.

The work explores this infrastructure protection problem area in more detail, and discusses several reasons why NYS may not be effectively evaluating and incorporating risk considerations during planning and design. The issues described as follows are

[6] Attributed to Winston Churchill; original source not found. GoodReads, "Never Let a Good Crisis Go to Waste," n.d., http://www.goodreads.com/quotes/717228-never-let-a-good-crisis-go-to-waste.

[7] Governmental systems include transportation systems, utilities, and support networks, such as emergency management systems.

present at the strategic, policy and operational levels. Although each section is presented individually, these issues interweave among each other, which can significantly complicate the problem.

1. Pitfalls of Reacting to an Event

Although some clear advantages exist to leveraging a tragic event, such as 9/11 or Hurricane Sandy, to affect change in infrastructure (both physical changes and policy changes), some problems can also arise. The ability to understand and evaluate risk can play an important role in identifying mitigation in the planning, engineering, and design phase. The first component of understanding risk is identifying threats. Although identifying all relevant threats could be most beneficial to the risk process, funds available to rebuild damaged assets may not allow for mitigation of threats not directly tied to the recovery effort underway.

The Metropolitan Transit Authority's (MTA) South Ferry Station was evaluated to demonstrate this issue. Although this example is being utilized to examine the challenges at hand, it is clear that in hindsight, it is easy to second guess decisions that were made in a very challenging environment. It is also acknowledged that the subway system had not faced a threat as extensive as Hurricane Sandy throughout its entire history. However, perhaps the same will be said for the next terrorist attack that could occur in NYS, and for that reason, stakeholders must continue to challenge the status quo to ensure the safety and security of the community.

As a result of the successful terrorist attack on September 11, 2001, in NYC, the subway system was significantly damaged.[8] This devastating structural damage wreaked havoc on the city. However, in the wake of this destruction, post-9/11 recovery funds provided an opportunity for the MTA to rebuild and enhance system capabilities.[9]

---

[8] Metropolitan Transit Authority, "Remembering and Rebuilding After 9/11," September 10, 2010, http://new.mta.info/news/2010/09/10/remembering-and-rebuilding-after-9-11.

[9] Metropolitan Transit Authority, "Restoring South Ferry Station," n.d., http://web.mta.info/nyct/service/RestoringSouthFerryStation.htm.

The new South Ferry Station, which opened its doors in 2009, was the pride of the subway system. It boasted improved operational capability, enhanced security features, and green building compliance. With 9/11 most certainly present and vivid in the engineer's minds, security was very likely a prioritized factor in the construction. With a $545 million dollar price tag, the threat identification and mitigation process could (and perhaps should) have also included a focus on flooding. A quick look at the existing 100-year flood zone maps visualizes this threat:

Figure 1. New York State 100-year Flood Zone Overlay[10]

The threat of flooding was known and relevant. The unknown question is whether or not it was included within the risk discussion—or at least to what extent it was addressed. However, it appears that the majority of components were not protected from

[10] Mapping Source: NYS Critical Infrastructure Response Information System; created by the author. This overlay visual demonstrates how South Ferry Station is located in a 100- year flood zone, which means a 1% annual exceedance probability exists.

the threat of flooding. With an anticipated $600 million dollar price tag, a commitment has been made to rebuild South Ferry Station in the wake of Hurricane Sandy. According to the MTA, "engineers are studying whether some of the vital electrical infrastructure can be moved to higher ground." Perhaps a start, but it should have been done prior to the first half billion-dollar reconstruction.

2. Risk Issues Addressing Man-Made Threats; Acceptable versus Unacceptable

Similar to the concerns described over the state developing a "tunnel vision" about recent or vivid threats, the issue of tunnel vision can also affect infrastructure owners/operators themselves. When infrastructure projects are approved to move forward, stakeholders intimately involved with the project begin a planning, engineering, and design phase that involves the consideration of many risk issues—ranging from financial risks (like cost overruns and insurance) to operational risks (like security and disaster response). Certain considerations and applications are simple, guided by standards and codes, which force the mitigation of risk for assets to be built in particular locales or for particular purposes. Obligations, such as those required for fire codes, communicate effectively that certain risks are considered unacceptable. The same can be said for standards and codes that deem certain building materials or techniques unacceptable for earthquake prone areas.

However, when security is considered with regard to man-made threats, discussions on acceptable risk are more uncertain. Individual owner/operators make judgment calls based upon the information and expertise available at the time of the infrastructure project conception and execution. Given the immense nature of the infrastructure environment, project stakeholders will most certainly utilize a variety of methods and processes to reach logical positions concerning the incorporation—or lack of incorporation—of security measures. In the end, decisions are made regarding infrastructure that supports the community and the construction budget, which often allow owners/operators to make the final determination in terms of the level of security risk they are willing to accept.

In some cases, infrastructure projects may miss the mark completely about one of the core components of evaluating risk in a comprehensive manner[11] (threat, vulnerability, and consequence[12]). Consider the following two basic examples in which the risk picture may be compromised in evaluating security considerations.

- A contractor is hired to assist with addressing physical security incorporation into the design of infrastructure. The contractor has a strong background in target hardening and applications, which could be applied through architectural design to mitigate consequences. However, the contractor relies on the owner/operator to communicate the threats to the facility. The designated individual on the project team tasked with developing the threat has no background in developing threat assessments and no analytical capabilities to research historical, current, and future concerns for the infrastructure type.
- A new asset is being built on a campus environment. Given the sensitivity of work and equipment planned to be located within the new asset, a comprehensive security team has been established to conduct a risk assessment for the asset to provide design guidance prior to architectural drafting. Although the team performs with a high-level competence, the project has ignored new vulnerability and consequences considerations for existing assets that will now be located adjacent to the new infrastructure.

The scenarios described above barely scratch the surface of the complexities and potential errors and omissions, which may occur during the planning, engineering and design phase. Like anything else, to expect a perfect outcome for every infrastructure project would be naive. However, to protect the interests of the community, government entities must be aware of these complexities and be prepared to step in and become a partner, which is especially the case when the owners'/operators' determination of acceptable risk could negatively affect public safety.

---

[11] Department of Homeland Security, "DHS Risk Lexicon," September 2008, http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf. The commonly accepted components of risk are threat, vulnerability, and consequence. Threat involves a process of evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations, and/or property. Vulnerability evaluates the physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. Consequence identifies the impacts or effect of an event, incident, or occurrence.

[12] Ibid.

3. Aging Infrastructure

In 2013, the American Society of Civil Engineers issued a report card highlighting infrastructure of concern for the nation and states.[13] Surveying a variety of infrastructure stakeholder organizations, the report demonstrates that many states, New York included, have some major infrastructure areas of concern that are in need of improvement. Several highlights specific to New York from the report are as follows.

- 39.6% of New York's bridges are structurally deficient or functionally obsolete.
- Drinking and wastewater investment needs are $56.7 million over the next 20 years.
- Public facilities have $96.5 million in unmet system and infrastructure funding needs.

As infrastructure—nationwide and in New York State—continues to face deficiencies and the risks of becoming obsolete, it becomes increasingly vulnerable to man-made and natural threats. Although a variety of reasons for these deficiencies arise from economic instability, weak oversight and more, the concept of the tragedy of the commons[14] summarizes the issues well. With a large portion of the aging infrastructure described above being publicly owned (including roads, bridges, waterways, etc), the community utilizes these assets and resources. Everyone within the community requires these assets to exist and society benefits from their presence; however, they generate little or no tangible profit despite the fact that costs do arise from their maintenance, and as such, it becomes difficult to maintain and/or improve them. Additionally, when opportunities arise to improve this infrastructure, a natural conflict over the scarce funding resources available occurs, which forces cost-benefit analysis to happen and priorities to be established.

[13] American Society of Civil Engineers, "Report Card for America's Infrastructure," n.d., http://www.infrastructurereportcard.org/.

[14] Garrett James Hardin and American Association for the Advancement of Science, *The Tragedy of the Commons* (Washington, DC: American Association for the Advancement of Science, 1968).

4. Uneven Focus on the Operational Life Cycle

Understanding that infrastructure has been a target of interest for terrorist organizations and other groups, as well as individuals with criminal intent, it is reasonable to see a focus placed on protecting this nation's infrastructure. However, overwhelmingly at the federal,[15] state, and local levels of government, available resources working to mitigate the risks associated with the terrorist or criminal threat are often focused on improving NYS's resiliency on assets within the operations and maintenance phase, and for the most part, overlook those entering the planning, engineering, and design phase.

Historically, the subject matter expertise (often physical security experts) that has been leveraged to assist with infrastructure protection lends its expertise well to analyzing and supporting the operations and maintenance phase. The most common occupations and careers held by professionals with physical security expertise are from the Department of Defense and law enforcement. These individuals have built their knowledge base around protecting and enhancing existing assets. Conducting assessments on existing infrastructure assets is natural for these individuals because it is familiar and what they have done on a routine basis. Security and risk analysis in the planning, engineering, and design phase do not fit comfortably with established infrastructure security personnel and processes. The planning, engineering and design phase requires conceptualizing an asset through drawings and discussions with architects and engineers. It requires new partnerships and planning methods to prepare the security discussion that often are not required for an asset that has already been built. These news partnerships and planning methods require formal adoption into the project processes and recognition at inception.

NYS has local assessment teams from large cities (New York City, Albany, and Syracuse), the NYS Office of Counter Terrorism Critical Infrastructure Protection Unit, as well as assigned protective security advisors[16] from the Department of Homeland

[15] This does not include General Services Administration.

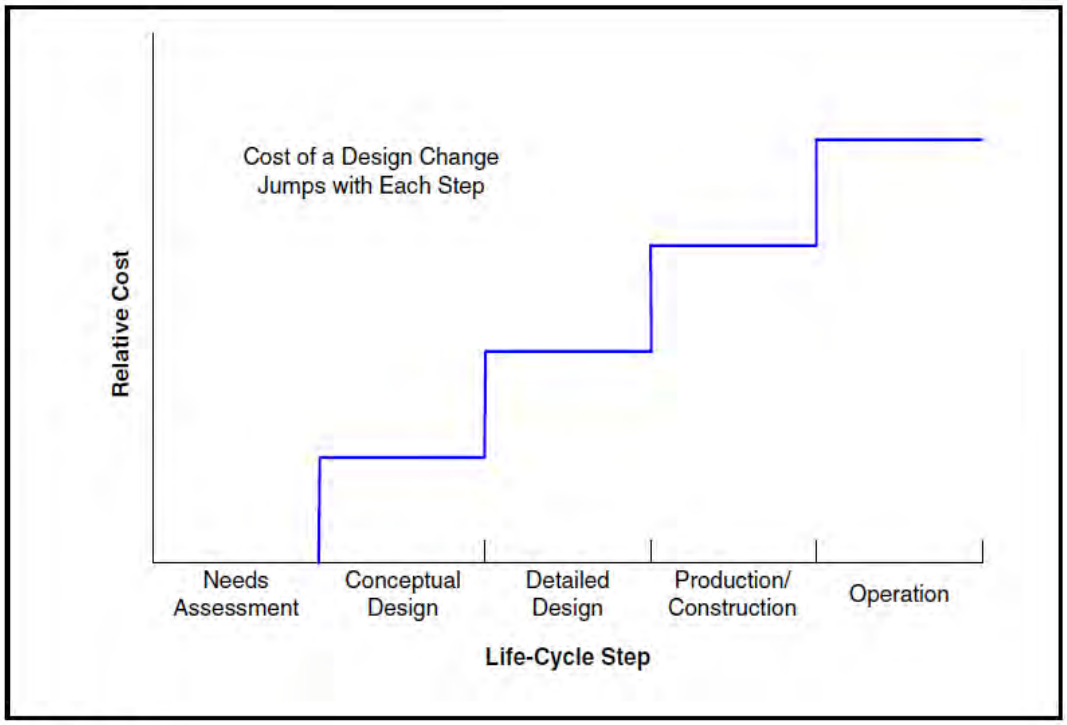
[16] Four protective security advisors are assigned to New York.

Security (DHS) all focused almost exclusively on existing infrastructure. Of the teams described, few are proactively positioning themselves for the collaboration and consultation that should occur as these new projects begin.

Finally, grant funds available to assist with the mitigation of risk for the infrastructure environment have also historically encouraged a focus on assets within the operational and maintenance phase. Grants, such as the federal Buffer Zone Protection Program, targeted existing assets, which met federal criteria to be considered significant. Additionally, national infrastructure prioritization programs encourage state and local efforts to work with, research, and justify existing infrastructure assets that would meet national criteria, which in turn, is utilized as part of the risk formula to allocate grant funds. These efforts do not consider infrastructure to be built or infrastructure about to begin a major reconstruction[17] phase. By recognizing issues with design early during the process, infrastructure funds will be saved and fewer mitigation efforts required once built. An example would be the incorporation of standoff for a building. Identifying the need for standoff distance during the conceptual phase of a project would simply require a new conceptual draft, which included a buffer zone between the parking lot and building. However, recognizing the need for standoff distance once the parking lot has been constructed would require similar redesign expenses and significant reconstruction costs. In a 2004 cost analysis study focused on interoperability, the National Institute of Standards and Technology provides a clear picture of the financial impacts recognized by an asset at different life-cycle steps (Figure 2).[18]

[17] Major reconstruction is defined for this thesis as projects, which change 40% or more of the asset.

[18] Michael P. Gallaher and Robert E. Chapman, *Cost Analysis of Inadequate Interoperability in the U.S. Capital Facilities Industry* (Gaithersburg, MD: U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology 2004).



Source: LMI.

Figure 2. Cost of a Design Change Chart[19]

Understanding the increased financial burden this nation's infrastructure stakeholders incur as their life-cycle progresses, coupled with what is understood about the relative nature of infrastructure, suggests the current heavily weighted focus of partnering with assets during the operational life-cycle is not the best application of limited resources.

All the aforementioned issues, and visualized in Figure 3, impact the overall infrastructure quality, which supports the community.

[19] Gallaher and Chapman, *Cost Analysis of Inadequate Interoperability in the U.S. Capital Facilities Industry*.

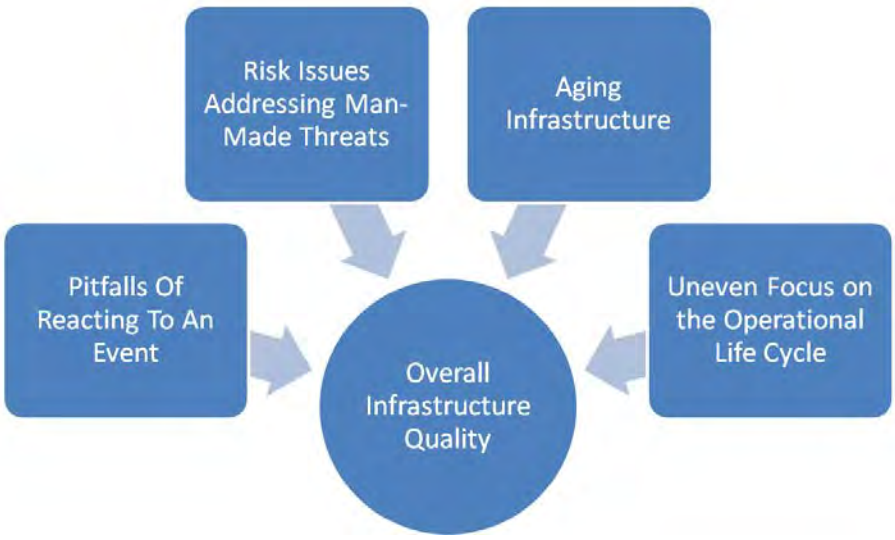


Figure 3. Infrastructure Protection Problem Space

Each issue on its own is complex, and if left unaddressed, could have negative long-term impacts concerning safety and security. Preparing stakeholders to participate effectively and efficiently in the planning, engineering, and design phase when the opportunity arises, may improve the state's overall resilience.

B. BACKGROUND

Important work has taken place historically to lower the risk associated with terrorism for NYS. Within the DHSES, the Office of Counter Terrorism (OCT), the Critical Infrastructure Protection Unit (OCT-CI) has developed goals to assist infrastructure stakeholders and protect the community. Although OCT-CI's organizational structure has changed several times, its mission and goals have remained consistent.

> The Critical Infrastructure Unit supports federal, state and local comprehensive risk analysis to reduce the Nation's vulnerability to terrorism and deny the use of critical infrastructure as a weapon by implementing plans and programs that identify, catalog, prioritize, and protect people and assets in cooperation with all levels of government and private sector.[20]

[20] Division of Homeland Security and Emergency Services, "Critical Infrastructure Protection Unit," n.d., http://www.dhses.ny.gov/oct/units/critical-infrastructure-protection/.

In support of this mission and in response to historical events, the NYS Legislature placed several mandates into law, which apply directly to the unit.

> NYS Exec Law Art. 26 §709 (j): Work with local, state and federal agencies and private entities to conduct assessments of the vulnerability of critical infrastructure to terrorist attack, including, but not limited to, nuclear facilities, power plants, telecommunications systems, mass transportation systems, public roadways, railways, bridges and tunnels, and develop strategies that may be used to protect such infrastructure from terrorist attack.
>
> NYS Exec Law Art. 26 §709 (k): Develop plans that may be used to promote rapid recovery from terrorist attacks and other natural and man-made disasters, to ensure prompt restoration of transportation, utilities, critical communications and information systems and to protect such infrastructure.

C. RESEARCH QUESTIONS

This thesis challenged the infrastructure protection status quo interpretation of the NYS executive laws identified above. Striving to obtain the ultimate goal of a resilient state, it will explore earlier opportunities for partnership and mitigation. To accomplish this outcome, two basic questions are asked.

- What are the benefits and challenges of NYS placing a greater focus on the planning, engineering, and design phase for new or majorly reconstructed infrastructure?
- How could a new partnership model at the state level be designed to support infrastructure protection activities during this phase?

Several key assumptions guide this research. First, infrastructure projects, no matter whether they are large or small, are complex and require significant collaboration and coordination with a multitude of stakeholders. Second, a natural pressure exists within all infrastructure projects concerning the customer-client relationship. No matter how genuine and committed to the greater good or success of the project, some stakeholders will be pressured to ensure a profit while others will focus on other societal goods; these sometimes conflicting pressures can negatively impact final outcomes. Third, this work addresses the concept of infrastructure at the macro level. It strives to examine infrastructure holistically, in an attempt to gain perspective and direction from which more detailed micro efforts could be born. Finally, when it comes to the safety and

security of citizens, NYS will ultimately be held accountable for its actions taken to protect its infrastructure from attack. Whether the infrastructure is public or privately owned will be insignificant, even if the constraints on protection efforts are vastly different.

II. LITERATURE REVIEW

A broad body of research—from public sector entities, practitioners, researchers and scholars—has been studied and written on these important issues. The most applicable and relevant analysis has occurred since 2001 because of the changing conception of security following the terrorist attacks of 9/11. This literature review focuses on that time period.

A. PUBLIC

Since 9/11, critical infrastructure protection has received a significant level of focus and attention. Guidance documents have been developed at various levels of government, and have in some cases, shaped the way infrastructure protection is accomplished. A seminal document for this practice is the *National Infrastructure Protection Plan (NIPP).*[21] Considered by many within the infrastructure protection community as a key foundational document, this plan provides a scalable framework for public partners to implement infrastructure protection activities.

While the NIPP does a thorough job identifying what components are required to assess risk (threat, vulnerability, and consequence), it does not consider that this nation's infrastructure is ever changing. Throughout the document, little consideration was given to what may be to come concerning new or majorly re-constructed infrastructure. Given how much infrastructure resides within the state that is in need of repair or modernization, this consideration is important. In this sense, the framework is a limiting, or at least limited, factor for those agencies attempting to begin infrastructure protection activities in their community.

Although the NIPP is the most updated and comprehensive national framework for infrastructure protection, it is certainly not the only plan, strategy, or other guiding document that can help in understanding the overall foundation of infrastructure protection. An important foundational document was published on infrastructure

[21] United States and the Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: U.S. Department of Homeland Security, 2006), 179.

protection called the *National Strategy for Physical Protection of Critical Infrastructure and Key Assets*;[22] similar to the NIPP, it provides guidance for infrastructure protection and a proposed path forward. Developed prior to the NIPP in 2003, this document developed a strategy, which included guiding principles and objectives to implement the Presidents *National Strategy for Homeland Security*.[23] Additionally, the State, Local, Tribal and Territorial Government Coordinating Council has published reviews by region of infrastructure protection programs that provide a greater understanding of how state and locals are implementing infrastructure protection activities on a regular basis. Information found within the *Final Report: Region VI Critical Infrastructure Protection Programs* provides significant information on local activities, best practices and challenges, and/or unmet goals. This information provides key insight into whether other state and local communities have considered operating within the planning, engineering and design life-cycle phase.

In addition to these documents, which have detailed frameworks and strategies, a review of more risk assessment focused documents provides a more detailed look at this environment. Similar to the NIPP, another work, such as the Building and Infrastructure Protection Series, provides a solid foundation.[24] This series of documents begins to address some of the more tangible aspects of infrastructure protection. One example is a document created in 2010 called *Aging Infrastructure: Issues, Research, and Technology*. This paper addresses concerns with the state of United States (U.S.) infrastructure and provides credible information on the need for new infrastructure and/or major reconstruction of existing infrastructure. Such documents demonstrate that NYS and the United States may be entering into a period of increased major re-construction and new infrastructure projects.

---

[22] United States and the Department of Homeland Security, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, DC: Department of Homeland Security, for sale by the Supt. of Docs, U.S. GPO, 2003), 83.

[23] Ibid.

[24] U.S. Department of Homeland Security, Science and Technology Directorate, "DHS Building and Infrastructure Protection Series Tools," n.d., http://www.dhs.gov/building-and-infrastructure-protection-series-tools-0.

B. PRIVATE

It would be naïve to assume that the private sector is not already including security considerations into their planning, engineering, and design life cycles. Literature suggests that architects and engineers are most certainly involving and including security into their curricula, advanced educations, and overall process recommendations. One example is a book developed by the American Institute of Architects called *Security Planning and Design; A Guide for Architects and Building Professionals*.[25] This book takes the professional through reasoning as to why a professional should incorporate security considerations, and walks the individual through examples of structural and non-structural physical security considerations.

As with the public sector, private organizations have also focused efforts on a more micro scale. Established as a not-for-profit organization; ASIS International[26] is one example of a large organization leveraged by the private sector and is committed towards advancing security for the community. ASIS is a professional association for security practitioners across a host of different industries. In addition to the certifications, which ASIS provides, it has a vast library of security and planning documents that provide a solid understanding of best practices and lessons learned. One example is the fifth edition of the Handbook of Loss Prevention and Crime Prevention.[27] This literature in many ways runs parallel to what exists in the public side, although with a focus on balancing security measures with other organizational priorities (like profits and controlling costs), and provides an excellent opportunity for review and comparison.

Another area with literature ripe for review is the area of whole building design,[28] a program of the National Institute of Building Sciences. Additionally, the American Institute of Architects has published a guide for a concept call Integrated Project Delivery

[25] Joseph A. Demkin and American Institute of Architects, *Security Planning and Design: A Guide for Architects and Building Design Professionals* (Hoboken, NJ: J. Wiley & Sons, 2004), 240.

[26] ASIS International, "American Society for Industrial Security," n.d., https://www.asisonline.org/Pages/default.aspx.

[27] "Research and Markets: Handbook of Loss Prevention and Crime Prevention: Edition No. 5," *Journal of Engineering* (September 26, 2012): 1245.

[28] National Institute of Building Sciences, "Whole Building Design Guide," n.d., http://www.wbdg.org/.

(IPD). IPD focuses on increasing the partnerships and efforts during early design to gain efficiency and effectiveness through the whole project. Similar to what the governmental programs have done, this private industry group has developed a framework for infrastructure professionals to assist them through the planning, engineering, and design phase. Included within this framework are sections focused on physical security, blast mitigation, and other structural aspects, which have relevance within the infrastructure protection world. In addition to literature available for review on this topic, the Institute provides case study examples for infrastructure, which have leveraged this information during the development of their assets.

C. PUBLIC-PRIVATE PARTNERSHIP

Any policy decisions made within this environment will warrant strong understanding and consideration of the public-private partnership. Issues, such as the challenges of sharing information and overcoming concerns related to liability, are examples of real problems, which are roadblocks to achieving a successful partnership.[29] Most recently in a response to Executive Order (EO) 13636, Booz Allen Hamilton described the issues about enhanced cyber security implementation as a lack of return on investment and an absence of intermediaries.[30]

Although this topic remains a challenge at all levels of government—with regards to identifying the best path forward—no lack of literature exists on characteristics for success and identification of core components. An article written by Fred Becker and Valerie Patterson focused on balancing returns, risks, and roles between the partnerships, which identifies positive association between risk and rewards as a key element for success.[31] Additionally, literature is available that focuses more specifically on this

[29] Sue Eckert, *Protecting Critical Infrastructure: The Role of the Private Sector,* Ridgway Center Working Papers, 2005.

[30] John McConnell, *Re: Notice of Inquiry—Incentives to Adopt Improved Cybersecurity Practices.* (Docket Number 130206155-3155-01) (Booze Allen Hamilton, 2013).

[31] Fred Becker and Valerie Patterson, "Public: Private Partnerships: Balancing Financial Returns, Risks, and Roles of the Partners," *Public Performance & Management Review* 29, no. 2 (December 2005), 125–144.

partnership and lessons learned on an international level, as seen within an article focusing on hospitals entering the contractual and design phase.[32]

D. EXPANDED PLANNING AND DESIGN EFFORTS

Finally, several works have been completed that align very closely with the topic and focus of this thesis. With 9/11 serving as a catalyst for efforts to improve overall security for high-rise buildings, the New York City Police Department (NYPD) published a document called *Engineering Security: Protective Design for High Risk Buildings*.[33] The document provides a structured guide as to how to "tier" an asset type (i.e., assess its risk level) and then apply specific recommended security considerations into the design of the asset. Additionally, it discusses and recognizes the struggle government and the private sector have concerning striking a balance between security and all the other administrative and operational focuses with which the private sector must deal.

The *Building Security Handbook for Architectural Planning and Design*[34] provides a comprehensive look at security in design and leverages a deep bench of subject matter experts to address the issue. Focusing on case studies from 9/11 and other recent events, the authors share lessons learned and discuss mitigation efforts that could be leveraged to make infrastructure more secure. With the majority of the work focusing on planning and design, different building types are explored in detail to provide best practices and security recommendations for each type. Additionally, focus is placed on the lack of codes relating directly to security, and how, in the absence of these codes, groups can leverage information that exists. Finally, this work reviews the fiscal issues related to implementing security in design and construction.

---

[32] Pedro Pita Barros and Xavier Martinez-Giralt, "Contractual Design and PPPs for Hospitals: Lessons for the Portuguese Model," *The European Journal of Health Economics* 10, no. 4 (October 2009), 437–453.

[33] New York City Police Department, *Engineering Security: Protective Design for High Risk Buildings*, 2009.

[34] Barbara A. Nadel, *Building Security: Handbook for Architectural Planning and Design* (New York, NY: McGraw-Hill, 2004).

The International Atomic Energy Agency (IAEA) utilizes a process at nuclear facilities called Design Basis Threat (DBT).[35] This process strives to evaluate the threats that could have high consequences and apply the appropriate levels of physical security protections to mitigate the identified threat.[36] Although the process is quite involved, two main components are emphasized. First a detailed threat assessment is completed, and second, an assessment and decision making process develops the DBT.[37]

Ultimately, this process assists the regulatory method with identifying allocation of resources. DBT offers a logical process for identifying attributes and characteristics of the adversary, which could be leveraged in the development of performance specifications.[38] Another benefit of utilizing DBT is that in addition to identifying threats that could have high consequences, it also excludes threats with minimal identified consequences.[39]

It should be noted that DBT has not come without controversy and critique over the process. In a recent review of DBT; Kuperman and Kirkham challenge its use of nuclear facilities and evaluate alternative methods.[40] Although options, such as game theory and improving the security culture are explored, they conclude that each option has its own issues and may not necessarily provide a higher quality output. However, the study did find that the DBT process should be made more rational.[41]

---

[35] International Atomic Energy Agency, "Implementing Guide, Development, Use and Maintenance of the Design Basis Threat," IAEA Nuclear Security Series No. 10, 2009, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1386_web.pdf.

[36] Ibid., foreword.

[37] Ibid., 13.

[38] Ibid., 21.

[39] Ibid., 22.

[40] Lara Kirkham with Alan J. Kuperman, "Protecting U.S. Nuclear Facilities from Terrorist Attack: Re-Assessing the Current "Design Basis Threat" Approach," *The University of Texas Blog Service*, August 15, 2013, blogs.utexas.edu/nppp/files/2013/08/NPPP-working-paper-1-2013-Aug-15.pdf.

[41] Ibid., 8.

III. METHOD

The methodology of this thesis is to apply a pragmatic qualitative approach using case studies to assess variations in assessment and cooperation frameworks. Recognizing the existence of the infrastructure protection problem area, the literature review was leveraged to determine what has been accomplished thus far within the infrastructure protection field in both the public and private realm focusing on planning, engineering, and design. Additionally, this review provided an informed understanding of the complexity of the planning, engineering, and design field. With this background, the research questions could begin to be addressed.

- What are the benefits and challenges of NYS placing a greater focus on the planning, engineering and design phase for new or majorly reconstructed infrastructure?
- How could a new partnership model at the state level be designed to support infrastructure protection activities during this phase?

To answer the first question, several public and private approaches were studied and analyzed, understanding the range of potential benefits and challenges could vary greatly. In recognizing the complexity of the infrastructure environment, three mini-case studies were selected to embody the infrastructure spectrum: simple government, complex government, and the private sector. The following entities were selected for the mini-case studies.

- U.S. General Services Administration (GSA): Representing the simple government approach, the GSA has control and authority of most federal buildings. The GSA implements a standardized and mandated program, which emphasizes incorporating safety and security in planning and design.
- United Kingdom (UK): Analyzed as the complex government approach, the United Kingdom has publicly available documentation focused on infrastructure protection that demonstrates a logical progression. This approach utilizes a voluntary participation approach.
- Whole Building Design & Design Build: Selected as the private sector approach, this approach has gained recent traction for infrastructure projects. NYS has authorized its use for several types of infrastructure

projects and is considering expanding the allowable scope. Additionally, privately owned infrastructure assets are utilizing the process as well. This approach utilizes a fiscal incentive participation.

This sampling provides a structured and focused comparison of public and private efforts utilizing various levels of complexity.[42] Throughout the review of these cases, the following questions were asked.

- What method is utilized to affect change?
- What are considered the key elements for success?
- Have smart practices[43] been identified?
- Are there known challenges and roadblocks that exist and remain unresolved?

The second question was addressed by focusing on the varieties of incentives for participation. Leveraging information collected in the mini-case studies. Potential participation incentives include voluntary, regulatory, and fiscally incentivized. Although not specifically associated with planning, engineering, and design, the infrastructure protection community has multiple programs and projects that correlate with the change agent methods identified during the first phase of this research. Programs and projects were selected for inclusion, review, and analysis if they have been utilized and/or leveraged in NYS and fit within one of the identified participation incentive categories. The goal of the analysis was to gain a broader understanding and knowledge base on participation incentive options and identify potential categorical strengths and weaknesses.

Finally, the research concludes with a recommendation that challenges the NYS infrastructure protection status quo and argues it should be restructured or re-conceptualized. To execute this alternative approach, a foundational plan was developed that assists NYS with addressing a segment of this problem. Additionally,

---

[42] George Alexander and Bennet Andrew, *Case Studies and Theory Development in the Social Sciences* (Cambridge, MA: Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, 2005), 71.

[43] Eugene Bardach, "Part Three: "Smart (Best) Practices"—Research: Understanding and Making Use of What Look Like Good Ideas from Somewhere Else," in *Practical Guide for Policy Analysis, The Eightfold Path to More Effective Problem Solving*, 4th ed. (Berkeley, CA: University of California, 2012).

recommendations for future research analysis required to continue to mitigate concerns related to the evaluation of risk and implementation of security measures for infrastructure are discussed.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. PUBLIC AND PRIVATE APPROACHES

Historically, within NYS, the security design component responsibilities of infrastructure projects have been left to the architectural and engineering contractors and interested/assigned employees from the owner/operator team. Although trained in applying best practices for safety and security, design teams can be placed in situations in which owner and operator requests, political ambitions, and funds available force difficult decisions and "trade-offs" to be made. Those that depend on this infrastructure, which will exist within the state for the long term, may benefit from enhanced collaboration approaches that explore in more depth the concepts of risk (threat, vulnerability, and consequences).

To discover how stakeholders could benefit from this enhanced focus, it is beneficial to look within and outside the continental boundaries to see how some organizations and groups are approaching planning and design. The literature review revealed three groups that have taken a proactive approach towards incorporating safety and security into planning, engineering, and design. The mini-case studies that follow provide insight into how these groups approach infrastructure protection. They demonstrate the American Society of Civil Engineers mantra: "The long-term viability of any Critical Infrastructure System—no matter how resilient and sustainable it is—will ultimately rely on the human and organizational stewardship the infrastructure system receives."[44]

A. SIMPLE GOVERNMENT: U.S. GENERAL SERVICES ADMINISTRATION

Although a large federal organization, the GSA was reviewed to represent a simple government approach, which for this thesis, is defined as an approach that has been developed to influence only the assets under its direct internal control. With the exception of Department of Defense facilities and a few other select departments, the

[44] ASCE Critical Infrastructure Guidance Task Committee, *Guiding Principles for the Nation's Critical Infrastructure* (Reston, VA: American Society of Civil Engineers, 2009), 40.

GSA is responsible for administering and managing federal agency space requirements.[45] Through this responsibility, it has been empowered with the control to administer and manage required programs. Through this charge, it is evident that it places a premium on planning, engineering, and design to ensure safe and secure properties and it is a stout steward for federal infrastructure.

With approximately $10 billion of work focused on new, major renovations, and other similar work, the GSA leans heavily on its concept of design excellence to ensure community funds are being spent in the best and most appropriate way possible.[46] Within its *Design Excellence Planning Guide*,[47] the importance and weight placed on collaboration becomes evident. Throughout the document, the GSA stresses that design excellence cannot be accomplished within a vacuum and must include a multitude of stakeholders and experts at various stages of the infrastructure project.

In addition to providing a design excellence framework for all contractors interested in building or rebuilding federal infrastructure, the GSA has also developed standards that must be followed. To achieve standards for safety and security, the GSA was supported by the Interagency Security Committee (ISC). Initiated by EO 12977 in 1995, the group has published standards and best practices, which serve as foundational tools for federal buildings. Examples of the standards most recently published, which are For Official Use Only (FOUO) documents, are the following.[48]

- March 2013/7th Edition—Design-Basis Threat
- March 2008/1st Edition—Facility Security Level Determinations
- April 2010/1st Edition—Physical Security Criteria for Federal Facilities

[45] General Services Administration, "Design and Construction Overview," n.d., http://www.gsa.gov/portal/content/104549?utm_source=PBS&utm_medium=print-radio&utm_term=HDR_1_Bldgs_design&utm_campaign=shortcuts.

[46] General Services Administration, *Design Excellence: Policies and Procedures*, 2004.

[47] Ibid.

[48] Department of Homeland Security, "Interagency Security Committee Standards and Best Practices," n.d., https://www.dhs.gov/interagency-security-committee-standards-and-best-practices.

The aforementioned titles demonstrate the logical progression and path this committee has created for federal buildings to ensure they are safe and secure. First, it has a standard that identifies and communicates the threat and is updated bi-annually.[49] Second, it has a process that requires an asset be placed into a security level. Third, standard security criteria have been established that correlate with both the design-basis threat and the designated security level for the asset, and are mandated for inclusion through planning and design.

These standards ensure components of the infrastructure project, which are non-negotiable, such as baseline security practices, are never excluded from incorporation into the final design. Additionally, the ISC develops supplemental best practices and training courses to encourage federal stakeholders to push the safety and security bar even further. Even with all this effort and success in mandating standards, challenges still exist.

One concern is that security can be taken too far and/or become inflexible. The Department of Defense may have been separated from the GSA's purview for this very reason. The *Guiding Principles for Federal Architecture* encourages accessibility, incorporation of fine art, and the development of landscape.[50] In May 2010, Barbara A. Nadel, FAIA, testified in front of the House Subcommittee on Economic Development, Public Buildings and Emergency Management concerning risk implications of applying Department of Defense standards in GSA lease procurements.[51] Representing the American Institute of Architects, she highlighted the importance of completing a detailed risk assessment for planned new facilities, and stresses the importance of flexibility in determining levels of protection based upon the specific variables that may present themselves for each project. Additionally, highlighted several times within the discussion

[49] Department of Homeland Security, "Interagency Security Committee Standards and Best Practices."

[50] U.S. General Services Administration, "Guiding Principles for Federal Architecture," n.d., http://www.gsa.gov/portal/content/136543.

[51] The American Institute of Architects, *Statement of Barbara A. Nadel, Too Much for Too Little: Finding the Cost-Risk Balance for Protecting Federal Employees in Leased Facilities, House Subcommittee on Economic Development, Public Buildings and Emergency Management*, May 20, 2010.

on risk assessment, Ms. Nadal focuses on the importance of "good intelligence" to inform "good design."

With "good design" as the goal, integration of all its components can be critical. When considering the many components that must be considered to protect from intrusion, blast, collisions, etc. the universe can become unmanageable.

> Security design is not rocket science, but for most building owners, design professionals, and public officials, integrating the many pieces of the security puzzle remains an increasingly challenging and complex art, one that can be mastered with proper guidance.[52]

Firm, steady, and artful guidance is what the GSA has incorporated into its organizational policy to protect its stakeholders.

B. COMPLEX GOVERNMENT: UNITED KINGDOM

The United Kingdom has been combating terrorism and exploring methods to reduce the overall risk to its infrastructure and community since the early 20th century. NYS has leveraged this experience and best practices developed to implement programs within the state to combat terrorism. Perhaps the most recognized example is the manner in which NYC developed and modeled the Lower Manhattan Security Initiative after the pre-existing "Ring of Steel" developed in London. This smart practice transfer demonstrates how groups do not have to create a completely new idea or concept; strong partnerships and information sharing can give new plans a warm start. Similarly, some examples of their focus on security and incorporating it into design are also present. This effort provides a look into a complex government approach.

Formed in 2007, the Centre for the Protection of National Infrastructure (CPNI) serves as one of the UK's resources for addressing infrastructure protection within its borders. Established as an interdepartmental organization, it is comprised of specialists from a multitude of relevant government agencies and services from both the public and private arenas. Similar to the homeland security focuses established within NYS and

---

[52] Terry Leach, "Federally Owned or Leased Office Buildings: Security Design," in *Building Security: Handbook for Architectural Planning and Design*, ed. Barbara Nadel (New York, NY: McGraw-Hill, 2004), 1.

much of the country, the UK's 2010 National Security Strategy placed particular emphasis on ensuring its infrastructure is secure and resilient.[53] It also recognized the need to improve collaboration and relationships between all levels of government and the public/private sector with regard to this subject matter area.

At first glance, CPNI and OCT-CI appear to be two parallel programs guided by homeland security strategies that are also in many ways aligned. However, their mission statements begin to show how their approach to tackling the challenges of infrastructure protection vary quite drastically.

OCT-CI Mission

The Critical Infrastructure Protection Unit supports federal, state and local comprehensive risk analysis to reduce the nation's vulnerability to terrorism and deny the use of critical infrastructure as a weapon by implementing plans and programs that identify, catalog, prioritize, and protect people and assets in cooperation with all levels of government and private sector.

CPNI Mission

Act as an interdepartmental organization providing advice on information, physical and personnel security to businesses and organizations across the national infrastructure

While both approaches could potentially lead to the same desired end state of protecting the community and its infrastructure, one acts as a change agent to the community through tangible and focused advice; the other leads a state effort by implementing plans and programs.

CPNI focuses its efforts and advice in three major areas: threats, security advice, and security planning. These areas are explored in more detail to understand how they are implemented.

[53] David Cameron et al., "A Strong Britain in an Age of Uncertainty: The National Security Strategy," *Stationery Office*, October 2010, http://www.cabinetoffice.gov.uk/sites/default/files/resources/national-security-strategy.pdf.

The National Risk Register[54] (NRR) serves as a backbone document for the UK and CPNI activities, and provides a clear explanation for infrastructure areas that have been and currently are priorities for focus. According to the Cabinet Office, the NRR lays out its "assessment of the likelihood and potential impact of a range of different risks that may directly affect the UK."[55] For each threat identified by the team of experts, the document provides a description and overview of the background, risk, and mitigation work that has been accomplished to address the issue. These threats are then weighed against each other to allow the reader to understand them in the context of relative impact and likelihood (Figure 4).

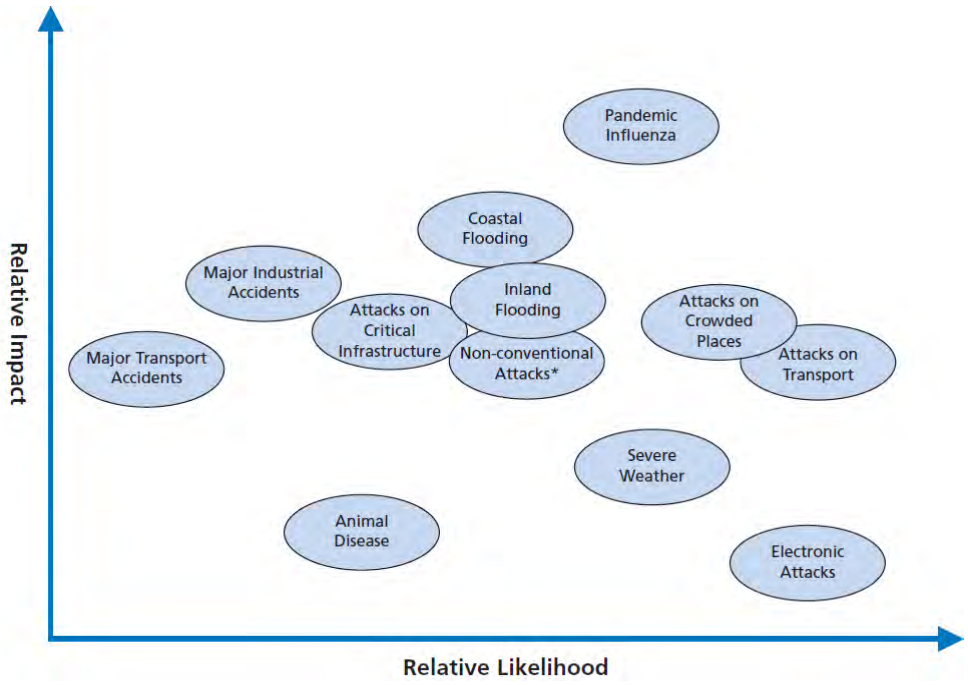


Figure 4. Graphic Showing Identified Threats from the NRR[56]

[54] Cabinet Office, "National Risk Register," 2008, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61929/CO_NationalRiskRegister_2012_acc.pdf.

[55] Cameron et al., "A Strong Britain in an Age of Uncertainty the National Security Strategy."

[56] Cabinet Office, "National Risk Register."

With a secondary goal of spurring debate and discussion on the accuracy of the assessment, the document provides transparency and comprehensive logic to the overall community concerning the threat picture. From this, the United Kindgom is then able to provide supporting documents, such as the National Risk Register for Civil Emergencies,[57] which explain in more detail how the community can better prepare itself for these threats. Finally, in support of CPNI activities, it more specifically provides a defined path from which to spend valuable resources to develop security advice to the communities in need of assistance.

Currently on its third addition, Protecting Against Terrorism,[58] serves as CPNI's macro approach to providing security advice to the greater infrastructure community. Leveraging a stakeholder community that has been informed and educated through documents, such as the NRR, this document begins the next level of education on how to counter these threats. Proposed as a starting point, CPNI devotes significant time and energy to providing advice and examples of best practices in the areas of protective security, response planning, and security culture.

Throughout the document, each section, whether focused on identification of vulnerabilities, development of site-specific plans, or understanding information security, provides understanding of what the topics is, why it is important, and how the individual or group can address the topic for their asset. Additionally, each section provides additional resources through which the stakeholders can learn more about the subject or take their actions to a higher level. Finally, a multitude of contacts and resources are shared with the reader to ensure the opportunity to follow up on outstanding issues or expand the knowledge base even further is available.

---

[57] Cabinet Office, "National Risk Register."

[58] Centre for the Protection of National Infrastructure, *Protecting Against Terrorism: 3rd Edition*, 2010.

Developed in partnership with the Department for Transport and the British Transport Police, Security in the Design of Stations (*SIDOS)*,[59] illustrates how CPNI provides advice at a more micro level within the community. An effort, which is clearly supported by the risk picture, SIDOS, takes a detailed look into the security of stations. Thus, the common theme and emphasis on design within CPNI becomes evident.

"Good design of the physical environment can reduce opportunities for crime, by making it harder to commit the crime."[60] Focusing its efforts on new or major redevelopments, CPNI and its partners utilize this document to ensure station stakeholders are investing their time and resources wisely and place the safety and security of stations to the forefront. Hence, the document reiterates that security must be an integral part of planning and design.

Similar to *Protecting Against Terrorism*, *SIDOS* provides the stakeholders a more detailed overview of the threat picture to their infrastructure. However, this document then becomes very detailed in the areas that should be addressed for stations, such as station approach, building structure, and fabric. Specific recommendations are made that provide what type of material should be utilized and the mitigation effect it will have.

As for most countries, although some great progress has been made in the area of infrastructure protection, the United Kingdom is not without issues and concerns within this area. The challenge of bridging the gap between relying on private industry to build and support much of the infrastructure and ensuring it is done in a safe and secure manner remains. Although the aforementioned overall process described takes the stakeholders through a logical path and progression, it remains voluntary and left to the infrastructure stakeholder's discretion as to whether they follow the guidance.

The challenges occurring at the Euston Terminal are an example of the ongoing issues.[61] With its last reconstruction completed in 1962 (and poorly done in many

---

[59] Centre for the Protection of National Infrastructure and British Transport Police, *Security in the Design of Stations Guide*, 2012.

[60] Centre for the Protection of National Infrastructure and British Transport Police, *Security in the Design of Stations Guide*.

[61] Ike Ljeh, "Euston, We Have a Problem," *Building.Co.Uk*, June 21, 2013, http://www.building.co.uk/euston-we-have-a-problem/5056620.article.

people's eyes),[62] this infrastructure was scheduled for a complete reconstruction to include the introduction of a high speed rail scheme (HS2). However, the complete redesign that would have included recommended security implementations as described previously was scrapped last year. With plans to leave the asset in its current state and simply add on the HS2 component, the safety and security concerns remain.

Detailed review of CPNI's infrastructure protection approach illustrates a program that has a clear mission and identified path to accomplish its ultimate goal of protecting the community and its infrastructure. Utilizing an integrated team of subject matter experts, CPNI can demonstrate to the stakeholder community its knowledge base and create specific work products (i.e., *Protecting Against Terrorism* and *SIDOS*) that relate to multiple infrastructure sectors. The United Kingdom has ensured its goal of providing security advice to stakeholders is first grounded by detailed threat assessment work. This step not only ensures the community is educated on the threats, but also understands why CPNI is focusing resources and partnerships on specific areas. In all areas in which consulting and guidance are provided, it ensures the information is explained, validated, and mitigation measures are offered. Finally, CPNI effectively partners and collaborates with other agencies to ensure the products are developed in a way in which actual recommendations can be made with confidence and supported by resource material.

Recent publications by CPNI, such as *SIDOS*, previously described, and other works, such as the Integrated Security; A Public Realm Design Guide for Hostile Vehicle Mitigation,[63] which addresses the threat of explosive devices and methods to design facilities to mitigate their effectiveness, demonstrate their focus on being a change agent prior to infrastructure being built or majorly reconstructed. Their role as advisor can be leveraged and utilized when the infrastructure is still conceptual. Understanding the potential long-term benefits, they champion concepts, such as crime preventions through environmental design and security by design. Thus, critical structural decisions, layouts,

---

[62] Jonathan Glancey, "Constructive Criticism: The Week in Architecture," *The Guardian*, 2011.

[63] Centre for the Protection of National Infrastructure, *Integrated Security: A Public Realm Design Guide for Hostile Vehicle Mitigation*, 2011.

and other key security protections can be implemented as part of the grand scheme and not added on later as an afterthought.

In concert with CPNI's efforts, the UK's Design Council, recently merged with the Commission for Architecture and the Built Environment (CABE), demonstrates another example for how serious and important the United Kingdom believes properly designed infrastructure is for its community. As part of their Design Out Crime initiative in 2011, the group produced a document sharing case study examples in which the best practices for design were utilized and successful around the world. Within the document, several success stories are provided for the United Kingdom.

One example is a major reconstruction project at Birmingham's Heartland Hospital.[64] Located in a dense urban area, this hospital struggled with preventing crime on its property. Benefiting from a safer hospitals initiative funded through the UK treasury, the hospital partnered with some experts on design and concepts, such as Crime Prevention Through Environmental Design (CPTED). Evaluating concepts championed by CPTED, such as increasing surveillance through natural line of sight and defining visitor traffic flow, an 80% reduction in trouble for the area of focus was identified. Additionally, the case study showed that overall, the employees felt more secure within the redesigned area.

Although the 2012 Olympics in London did include some significant security concerns and gaps, most notably, the contract issues for private security guards and the inability to provide the personnel promised. The planning and construction for this event provides another example for how the United Kingdom has been able to put the security design concept into practice. Focusing heavily on temporary facilities, CABE provided its services and input with regards to design guidance on a multitude of venues to include the hockey facilities and Olympic Park.[65]

---

[64] Home Office Design and Technology, Alliance Against Crime and the Design Council, *Design Out Crime: Case Studies, Examples of Design Being Used to Tackle Crime Problems Around the World*, 2011.

[65] Commission for Architecture and the Built Environment, "London 2012 Reviews," n.d., http://webarchive.nationalarchives.gov.uk/20110118095356/http://www.cabe.org.uk/design-review/london-2012.

The complexities that exist within the infrastructure protection environments can be quite overwhelming. Through a review of some of the UK's efforts, it is clear those problems, such as creating an effective public/private partnership model, cross international borders. However, their use of being a change agent through the development of an interdepartmental organization and providing focused advice are promising infrastructure protection design steps.

C. PRIVATE SECTOR: WHOLE BUILDING DESIGN AND DESIGN BUILD

Private industry has also taken steps forward on its own to advance the bar for safety and security concerning planning and design. Within the infrastructure environment, frameworks and organizations are being developed around concepts, such as design-build and whole building design. Although utilization of these tools and processes is voluntary, they carry with themselves fiscal incentives and savings that serve to entice new users. These concepts form a strategy and process to encourage excellence.

The design-build concept approaches infrastructure projects from a non-traditional contracting direction. The Design-Build Institute of America summarizes its process as "…an integrated approach that delivers design and construction services under one contract with a single point of responsibility."[66]

Unlike normal building design and contract practices, which shift responsibility between contractors as the project progresses, design-build keeps the responsibility under one united contract. Figure 5 shows how concepts like design-build are steadily growing and supported in the community of non-residential housing construction.

[66] Design-Build Institute of America, "About," n.d., http://www.dbia.org/Pages/default.aspx.

Use of Design-Build Delivery Method on Projects Above and Below $10 Million

YEAR	VALUE	Dollar Value Market Share
2005	Above $10 Million	0.376
2006	Above $10 Million	0.375
2007	Above $10 Million	0.421
2008	Above $10 Million	0.455
2009	Above $10 Million	0.490
2010	Above $10 Million	0.525
2005	Under $10 Million	0.203
2006	Under $10 Million	0.209
2007	Under $10 Million	0.209
2008	Under $10 Million	0.235
2009	Under $10 Million	0.243
2010	Under $10 Million	0.248

Figure 5. RCD/RSMeans Market Intelligence Graph[67]

The design-build structure provides an opportunity for collaboration to occur within a planned framework and offers a defined methodology, which aims at improving a multitude of characteristics of the build. Within NYS, the use of design-build has progressively increased. Through the NY Works program, this concept is being communicated as the best path forward to rebuild the states infrastructure ensuring expedited development, reduction of overall costs, and all for "value engineering."[68]

The Kosciusko Bridge Project is a recent example of its use in NYS.[69] Leveraging federal and state funding, certified design-build teams are competing for the contract award to build a new bridge connecting Brooklyn and Queens. During this

[67] Reed Construction Data/RSMeans Market Intelligence, *Design-Build Project Delivery Market Share and Market Size Report*, 2013.

[68] New York State, "NY Works," n.d., http://andrewcuomo.com/nyworks.

[69] NYS Department of Transportation, "Kosciuszko Bridge Project," n.d., https://www.dot.ny.gov/kbridge.

process, pre-qualified bidders will develop detailed proposal that communicate and consider all the required elements to build the required bridge. This process will require bidders to communicate how the planning, engineering, and design concept developed by their team will withstand safety and security considerations developed by the NYS Department of Transportation.

A program within the National Institute of Building Sciences, the Whole Building Design Guide,[70] demonstrates another platform focused on planning and design. A major goal is to ensure high levels of collaboration and coordination occur early in the planning and design phase. More specifically, the Whole Building Design Guide[71] suggests that to design a safe and secure building effectively, it must be considered within a "total project context." Utilizing multi-disciplinary teams, the proposed design must be evaluated against all relevant hazards the future asset may face.

Core to this process is the need for the owner/operator to designate an owner's representative. Within an environment that lacks clear standards, such as those developed by the GSA, this individual ensures all design work is in line with the owner/operators' expectations and needs. This individual becomes the assets steward for the process flow described as follows.

[70] National Institute of Building Sciences, "Whole Building Design Guide."

[71] Ibid.

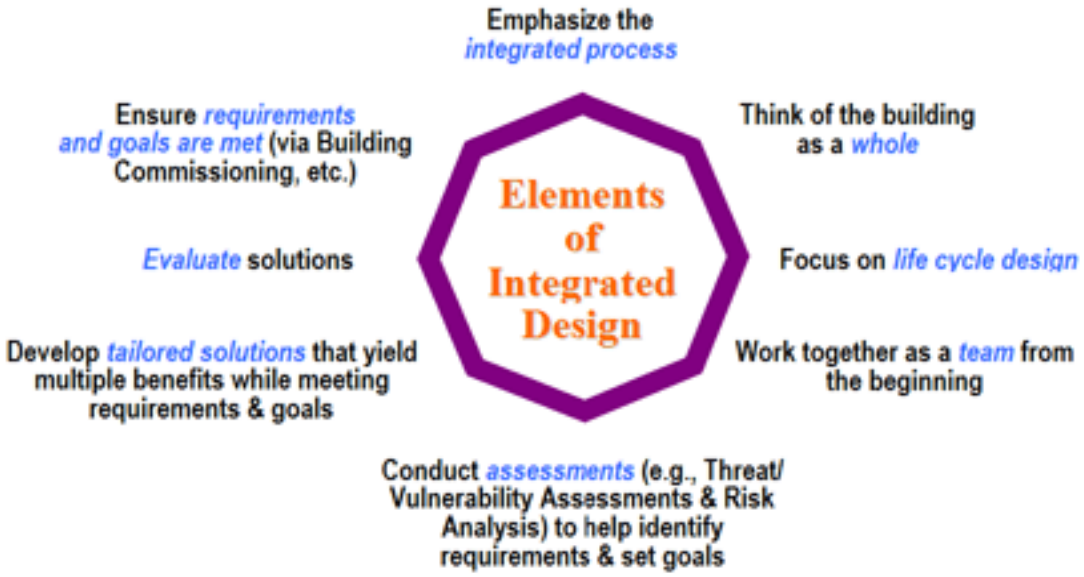


Figure 6. Whole Building Design Flow Chart[72]

As visualized through the chart in Figure 6, in several critical areas (conduct assessments, develop tailored solutions, evaluate solutions), the inclusion of intelligence-based analytical component and knowledgeable physical security expertise would be helpful to inform decision making. If these components are not incorporated early into the planning, engineering, and design phase, and are left until the review requirements portion of the process, the inclusion and/or consideration of these safety and security components will at best be band-aids to resolve the issue. In a worst-case scenario, issues that may have been possible to mitigate earlier within the planning phase may not be possible at all due to the final asset design.

EPA Region 8 Headquarters provides an example of a new construction asset that utilized the process of design-build and whole building design.[73] With a project team of approximately 11 people, the group established goals for areas such as the following.[74]

- Secure/Safe

[72] WBDG Aesthetics Subcommittee, National Institute of Building Sciences, "Engage the Integrated Design Process," Last updated November 5, 2012, http://www.wbdg.org/design/engage_process.php.

[73] National Institute of Building Sciences, "Whole Building Design Guide."

[74] Ibid.

- Sustainable
- Functional
- Accessible
- Aesthetic
- Cost-Effective
- Historic Preservation
- Productive

Leveraging the Whole Building Design Guide flow, multiple teams were established to accomplish these goals; however, integration and communication were important factors in achieving the goals.[75] An important lesson learned shared from the project was that "Design-Build and design excellence should not be mutually exclusive."[76] The project also highlighted that if local stakeholders had been integrated earlier within the process, several unachieved goals may have been realized.

Both The Design-Build Institute of America and The Whole Building Design Guide are non-governmental organizations, which serve to improve overall building design. They exist, however, due to the funding provided by contract awards (public and private) and other government funding. This fiscal incentive drives competition, which encourages solutions that benefit the infrastructure community.

D. AGGREGATED ANALYSIS

Although the approaches reviewed above vary concerning their role within the infrastructure community, each demonstrated a clear interest in enhancing safety and security through planning, engineering, and design. This common objective of desiring to influence changes during planning, engineering, and design demonstrates the significance of this phase. In addition to this common objective, several other similarities were identified.

First, each approach established a process that would encourage early participation of the identified stakeholders. Allowing the safety and security discussion to

[75] Ibid.

[76] Ibid.

be incorporated at a later phase of the planning, engineering, and design cycle, is not encouraged by many working at the cutting edge of this field in both the public and private sectors. Second, the concepts of integration and collaboration are present within each approach. Eliminating stovepipes and encouraging open discussion among different types of subject matter experts appears to be valued in each approach, despite their differences. Finally, although the path taken to identify expectations varied, each approach clearly identified its safety and security expectations, and worked to incorporate them into the project. Establishing a benchmark and/or standard for safety and security expectations allows participants to evaluate their progress and ultimate success throughout the planning and design phase.

In addition to having commonalities, this review also brought to light differences among these approaches. Based upon their position and role within the infrastructure community, the approach naturally must vary to be effective. A private sector approach would likely be ineffective when attempting to apply a mandated incentive for participation as demonstrated by the GSA, simply because it is optimized for participants with differing sets of incentives. Likewise, it would be of less value for the GSA to utilize a purely fiscal incentive for its planning and design efforts since it already has control and ownership over its assets from start to finish. These nuances surrounding participant incentives become a very important consideration that must be evaluated and studied prior to implementing any new program. After all, if an organization developed an approach that would most certainly enhance safety and security, yet could not be effectively implemented through the group's sphere of influence, little would be accomplished.

V. VARIETIES OF INCENTIVES FOR PARTICIPATION

The aforementioned planning and design approaches demonstrate that within the infrastructure protection environment, varying levels of relationships and partnership exist. Perhaps the least complicated one (yet not without its issues) is the public-to-public infrastructure relationship. On the other hand, the most challenging is the public-to-private infrastructure relationship. Many of these interactions are created or fostered by governments to affect change within their identified community of interest. To accomplish their various missions, governments have developed a range of solutions. These solutions vary from strictly voluntary to fiscally incentivized, as well as regulatory/mandatory programs. These options are explored in detail to understand the benefits and challenges that come with each.

A. VOLUNTARY PROGRAMS

Voluntary programs are utilized at multiple levels of government within the infrastructure protection community. Within the DHS, their Office of Infrastructure Protection offers multiple partnership opportunities to infrastructure stakeholders. Utilizing products like their Infrastructure Survey Tool (IST), Site Assistance Visits (SAV), and Computer Based Assessment Tool (CBAT), stakeholders are encouraged to open their doors and share detailed information, which can bring to light vulnerabilities and provide options for consideration to mitigate them. At the state and local level, similar programs exist to attempt to accomplish the same end state, more resilient infrastructure. Two examples of these efforts are the Initial Asset Visit (IAV) and Enhanced Visual Assessment Program (EVAP). These programs reflect a similar approach as described previously for the IST and CBAT, respectively.

However, it is ultimately left to the sole discretion of the owners/operators as to whether they implement any of the recommendations provided by these voluntary programs. Understanding the cost burden recognized by including security enhancements, these partnerships often look for low cost, no cost solutions that are less problematic to implement, which does not necessarily mean however that these low cost,

no cost solutions are the highest priority mitigation recommendations. In some cases, major vulnerabilities identified are so cost prohibitive they simply must be recognized as existing and it is understood that a realistic mitigation option is not available. Very simply, the profit requirement will often stifle change. Often, these programs also provide owners, operators, or security personnel with "evidence" (i.e., outside assessments) to show their organizational leadership so that they may advocate on behalf of new or expanded security measures.

At a minimum, these partnerships carry the safety and security torch forward to foster communication on the important topics and likely educate owner/operators on important vulnerabilities to consider. Additionally, as owner/operators provide information on their assets to receive final products, the government is compiling a large database of information on infrastructure and utilizing it to inform decision makers about this topic. However, the question remains; is enough value provided on its own to justify the expenses of these programs?

B. FISCALLY INCENTIVIZED PROGRAMS

Whereas regulatory and mandated programs could be referred to as utilizing "the stick" method, fiscally incentivized programs could be referred to as utilizing "the carrot" method. This type of incentive occurs both in the public and private sector and both areas are explored in this chapter. This approach works under the assumption that infrastructure owners/operators desire to implement safety and security mitigation measures; however, due to constraints (fiscal, personnel, time, etc.), they are unable to, which can nonetheless be accomplished through both direct and indirect approaches.

Grant programs developed and/or managed by FEMA play a key role in providing an incentive for change. Two major programs, which come from FEMA, are the Fiscal Year 2013 Homeland Security Grant Program (HSGP) and the Fiscal Year 2013 Hazard Mitigation Grant Program (HMGP). While both programs strive to create a more resilient nation, the HMGP maintains a strict focus on natural hazards while the HSGP expands its focus towards not only terrorism but also other catastrophic events.

With $354,644,123 total funding available, the State Homeland Security Program (SHSP) is the core program housed within the HSGP. Requiring the submission of investment justifications, threat and hazard identification, and risk assessments and other supporting documentation, the program strives to assist with the following areas.[77]

- Planning
- Organization
- Equipment
- Training
- Exercise

Following the aforementioned guidelines, State Administrative Agencies (SAA) distribute fund directly to local entities, create sub-grant programs, and utilize the funds for state needs. Although this process affords flexibility in many respects, FEMA does restrict and manage what is considered allowable expenses. An example is the authorized equipment list.[78] This list provides funded recipients a guide to determine if the equipment they wish to purchase is allowable under the program policy. Additionally, restrictions prevent the expenditure of funds on privately owned infrastructure.

Alternatively programs, such as the HMGP, focus their efforts solely on natural hazards. In addition to the focused nature of mitigating threats, local entities are eligible to apply for the grant and compete for funding. Applicants must walk through a very detailed application process that communicates how they have addressed elements such as the following.[79]

- Mitigation Planning
- Technical Feasibility and Effectiveness
- Floodplain Management and Protection of Wetlands
- Environmental Planning and Historic Preservation Review and Compliance

---

[77] Federal Emergency Management Agency, "FY 2013 Homeland Security Grant Program," n.d., http://www.fema.gov/fy-2013-homeland-security-grant-program-hsgp-0.

[78] Federal Emergency Management Agency, "Authorized Equipment List," n.d., https://www.rkb.us/mel.cfm?subtypeid=549.

[79] Federal Emergency Management Agency, *Hazard Mitigation Assistance Unified Guidance*, 2013.

- Cost-Effectiveness
- Cost Review

Although this process ensures stakeholders are approaching mitigation planning methodically and logically, the narrow focus on natural hazards can lead to planning and design flaws as described earlier within the problem area. While assisting in mitigation of certain threats, the program also encourages tunnel vision.

Finally, fiscally incentivized tools can also be more indirect than grant programs. Leadership in Energy & Environmental Design (LEED) is a recent and successful example of this type of tool. Established as a third party tool to encourage the use of "green buildings," the programs provide standards and a certification process to guide interested parties through the process of conserving energy, utilizing space effectively, and using natural resources appropriately.[80] As a reward for certifying through this process, benefits include lower long-term operating costs, tax benefits, and zoning allowances.

While improving energy efficiency and limiting the damage industry can do to the environment, programs, such as LEED, can have a negative impact on safety and security. An example would be the utilization of windows. Windows allow buildings to take advantage of the heat provided by the sun and limit the amount of artificial heat required to sustain a building. However, when concerned with the threat of an improvised explosive device, windows on a building provide little protection from an attack and can become secondary projectiles and cause additional injuries. Finding a balance between being "green" and secure can be quite challenging, even something as simple as the use of outdoor lighting at night can cause conflict.[81]

C. REGULATIONS AND MANDATORY PROGRAMS

The use of regulations and mandatory requirements to accomplish goals and affect change has also been utilized at all levels of government in the infrastructure

[80] U.S. Green Building Council, "Leadership in Energy & Environmental Design," n.d., http://www.usgbc.org/leed.

[81] Laura Spadanuta, "The Greening of Security," *Security Management*, n.d.

sphere. Over history, the use of building codes has been widely accepted and implemented for fire protection, public health, and engineering, yet no comparable set of security codes exists.[82] As described earlier, at the federal level, mandatory criteria and standards have been adopted to bridge the lack of security codes. However, many state and local government organizations have not attempted anything similar.[83] It is not difficult to understand why an overarching security code has not yet been realized, as risk levels are context specific and not universal. The threat posed to the community by man-made attacks is an intelligent, flexible, and multipronged one, and a far less common one than, for example, the risk of fire. Codes that have been adapted to mitigate risks created by natural hazards do not have to concern themselves with a selective and adaptive foe. It is simple to justify their implementation because anyone could be affected without requiring the justification of threat information.

Another form of regulation seen within the infrastructure community comes from the oversight role, most common with sectors seen as "utilities." This type of regulation exists in areas, such as the energy sector. Certain community services are considered by the government to be so crucial for the community that regulations must be placed on providers to ensure continuity and quality. This focus aims to ensure services are provided to the community at an appropriate cost, and that enough resilience is built into the system that it can withstand common and likely hazards. This type of regulation is also seen on infrastructure, which could prove harmful to the community by its improper use or obtained with malicious intent through theft and diversion—like in the chemical or nuclear sectors. Unlike the voluntary programs, these regulations and mandates can carry an operational and/or fiscal penalty, which forces the hand of the owner/operator to maintain compliance with the required rules. In this regard, desired changes, which are implemented through regulation or mandate, can be very effective.

However, regulations and mandates are not without problems. A recent example demonstrating some of the problems that can develop is the Chemical Facilities Anti-

[82] Walter "Skip" Adams and Deborah A. Somers, "Codes, Standards, and Guidelines for Security Planning and Design" in *Building Security: Handbook for Architectural Planning and Design*, ed. Barbara Nadel (New York, NY: McGraw-Hill, 2004), 3.

[83] Ibid.

Terrorism Standards (CFATS) program within the DHS. Created by government to improve security at facilities with dangerous chemical, serious questions are being raised about their ability to implement the program effectively.[84] Programs, such as CFATS, require a large office to manage and operate the program with taxpaying dollars funding the efforts.

Most recently, an explosion at a fertilizer plant in Texas demonstrates the gaping holes that can exist within these programs. This plant carried quantities of ammonium nitrate that clearly fall above the threshold amounts that should have placed them under CFATS control and required submission of security plans and inspections; however, the last time the company had a federal inspection conducted was 28 years ago.[85] Outliers, such as this plant, can fall through regulatory cracks for many reasons including but not limited to the failure to self-identify themselves, improper communication of chemical inventories, and limited inspection resources focused on higher tiered assets. Whatever the reason may be for the asset slipping through the cracks, it demonstrates the fallible nature of regulations and mandates.

Such regulatory approaches are also far more coercive than those relying on financial incentives or voluntary participation. Both economic (among owners/operators) and ideological or philosophical (among those opposed to government intervention in markets) have caused objections to such regulations. In both cases, these reasonable objections must be taken very seriously and balanced with community needs and other values like resilience.

D. SYNTHESIS

Each aforementioned participation model discussed has multiple sub-layers that provide options for consideration when striving to accomplish a desired outcome. While approaching a complex matter, such as infrastructure protection, it is unlikely that one solution solves the safety and security problem on its own. It is more likely that multiple

[84] U.S. House of Representatives Chairman Fred Upton, *Congressional Leaders Express Reservations about Extending CFATS Funding in Light of Program's Failures*, Energy & Commerce Committee, 2013.

[85] Adam Estes, "The Exploding Fertilizer Plant in Texas Hadn't Had a Full Inspection in Three Decades," *The Atlantic Wire*, 2013.

methods and models are required to be utilized and interwoven amongst each other. Concerning incorporating safety and security into planning, engineering, and design, stakeholders should consider their role within this community and evaluate their capabilities to affect change.

The participation models reviewed previously each carry with them an intrinsic coercion value. An increasing coercion value for a well-managed and executed program has a greater likelihood of achieving the goal established. Figure 7 is a basic representation of this increasing coercion value.

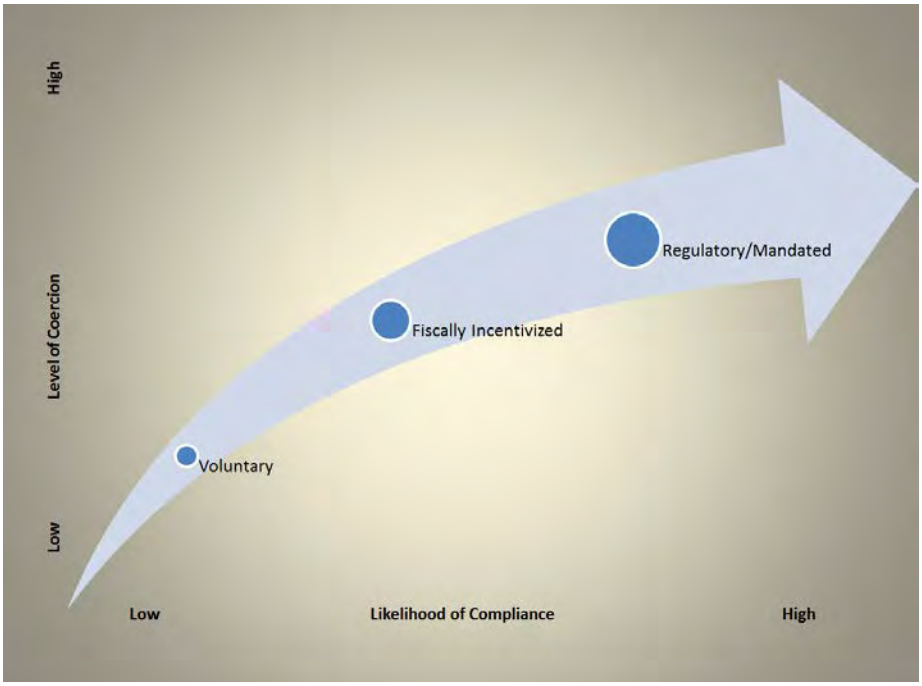


Figure 7. Coercion Value Scale to Accomplish Desired Outcomes

It should be noted (as discussed in several examples earlier) that although the coercion value can impact achievement of a desired goal, it is not the only required value to consider. A poorly managed and executed regulatory program may cause more harm than good and be less effective than a well-executed voluntary program. Additionally, regulatory programs impose costs on industry, and owners/operators, and at a certain point, such costs may outweigh the "upside" of increased security. However, a well managed and executed regulatory or mandated program can accomplish the desired goal.

The review of the GSA and its development of a mandated safety and security program demonstrates how such a program can be effectively implemented. Leadership determined that safety and security measures must be incorporated into federal buildings; a team was designated to develop a logical process to accomplish the directive, standards were issued, and oversight was established to ensure the standards were being followed.

VI. NEW MODEL FOR NEW YORK STATE

Recognizing DHSES's place in infrastructure protection within NYS, the following proposal is a new approach to improve safety and security for the state's infrastructure and the community that relies on it. This plan will not address all infrastructure sectors and assets within the state; it will focus on areas over which the state has authority and/or significant influence. A goal is to interweave new approaches that improve the aggregate and mitigates safety and security risks within this setting. Below are two new approaches for the state to consider for implementation. Both approaches would be tailored to address new and majorly reconstructed infrastructure.[86]

A. STATE OWNED AND LEASED INFRASTRUCTURE

Similar to the GSA at the federal level, the Office of General Services (OGS) is responsible for the management and administration of state owned buildings within NYS. To accomplish this task, the OGS has several groups that include but are not limited to building administration, real estate services and design and construction that share these responsibilities. Currently, within the OGS, mandated security standards for state owned buildings do not exist. Although within the building administration group, a security and emergency management unit exists to assist with security projects,[87] and several state agencies have developed their own standards,[88] the inclusion of security elements within buildings remains voluntary.

1. Recommendation

NYS should develop and publish standards with which any new or majorly reconstructed state owned buildings are required to be in compliance. Additionally, these standards should include requirements for leased state buildings. If NYS is to begin to

[86] Majorly reconstructed infrastructure for this plan is defined as total or partial replacement of structure; not including a sum of partial replacement totaling less than 40 percent.

[87] Office of General Services, "Security and Emergency Management Unit," n.d., http://ogs.ny.gov/BU/BA/SEMU.asp.

[88] Ibid.

champion the concepts of incorporating increased levels of safety and security into the planning, engineering, and design phase, it must start internally. Albert Einstein once said, "Setting an example is not the main means of influencing another, it is the only means."[89]

2. Benefits

By implementing standards for new buildings, ones that will be undergoing major reconstruction and new lease agreements, the state could begin an incremental process of improving safety and security at state owned and leased buildings. This method for change would ensure progress is made without shocking the system that would require all existing assets to comply with a new standard.

The participation incentives analysis demonstrated that if the development of mandatory programs is possible, this form of influence can be the greatest. Additionally, with the OGS having similar roles and responsibilities as the GSA, the simple government approach developed by the latter could likely be leveraged to begin the development of state standards and practices. The GSA has demonstrated excellence within this field and has developed a method to provide flexibility that would also be needed in NYS.

3. Challenges

The first major challenge faced is persuading the OGS leadership and state leadership to move forward with the recommendation. Switching from a voluntary practice to a mandatory one, which would impact most state entities including imposing real costs on them, will likely face resistance. Major factors for resistance may include the following.

- Fiscal Concerns: Although incorporating improved security measures during planning and design is less costly than doing so once an asset has been built, it remains an expense. Any increased expenses for state owned assets will likely be challenging for agency budgets and plans. NYS, like states across the country, remains in a challenging economic environment and concerns over increased spending cannot be overlooked.

[89] Glenn Van Ekeren, *Words for all Occasions* (Rowe, MA: Prentice Hall, 1988), 234.

- Relinquishment of Authority: With the inclusion and implementation of security measures delegated to the individual agency, individual leadership groups may be hesitant to relinquish that authority. Leadership may view it as a less beneficial process than their previously developed internal policies. Most mandatory policies face resistance from those to whom they limit the discretion.
- Perceived Lack of Threat: Although NYS has been the subject of terrorism attacks in recent history, the vast majority of NYS owned assets have not been successfully attacked. Agency leadership may argue that the overall risk to the state does not justify the need to develop and implement standards.

Another challenge faced is the development and execution of the proposed standards. As previously discussed, a mandated program is only successful if it is developed and executed well. Development and execution of this recommendation will require personnel commitment from multiple agencies to develop, publish, implement, and update—as well as the creation of a training program to share such standards with relevant agency stakeholders.

4. Next Steps

To begin forward movement on this recommendation, DHSES leadership should meet with OGS leadership and representatives from the Governor's office to discuss any proposed change. The path towards implementation could be recommended in three phases and address challenges described previously.

First, the existing OGS, Security and Emergency Management Unit, could be charged with developing draft standards that could be considered for approval and use on state owned and leased buildings. Leveraging this unit would likely relieve some of the concerns related to the relinquishment of authority as this group is already established and is charged with protecting personnel and structures under the OGS's control.[90] To accomplish this task, the DHSES would assign personnel to assist the unit and its existing membership. A primary requirement of this group would be to determine the scale and scope of what "state owned and leased buildings" should include. A major role for DHSES within this group would be to develop threat briefings, present on, and inform

[90] Office of General Services, "Security and Emergency Management Unit."

agency leadership about threat picture for NYS owned buildings. Additional preliminary requirements would include the development of stakeholder outreach and communication methods, fiscal impact studies, as well as of a plan to update leadership regularly on progress.

Second, once the preliminary work is completed and approved by leadership, the unit and supporting membership will draft standards to be applied to new buildings, buildings undergoing major reconstruction, and leased buildings. This approach would allow the state to incur the additional expenses related to improving safety and security gradually, and not overburden an already constrained fiscal environment. As demonstrated by the GSA, these standards should include three core components: design basis threat, facility security level determinations, and physical security criteria. Once drafted, opportunities should be provided to all interested agencies to review and comment on the draft standards.

Finally, once approved and provided to all agencies, the unit should maintain oversight on implementation of the standards. Ensuring compliance with the standards will be an important element to ensure success. Additionally, the standards should be reviewed and updated on a yearly basis as necessary to ensure they are current and address the threats that NYS faces.

B. STATE FINANCED INFRASTRUCTURE

Another area in which NYS has direct influence on new or majorly reconstructed infrastructure is through financial support. A recent example is under the NY Works program championed by Governor Andrew Cuomo, in which an effort is underway to "rebuild NY's infrastructure."[91] Leveraging an aggregate of available federal and state funds, the group will earmark resources to support economic development or transportation infrastructure projects.[92] Throughout this research process, it has been demonstrated that "good intelligence" and establishing a baseline threat picture is

[91] New York State, "NY Works."

[92] Ibid.

important to the planning and design process. Through the utilization of such fiscal incentive participation tools, enhanced safety and security processes could be attached as a requirement for selected projects.

1. Recommendation

Where NYS funds are provided to assist with the creation of a new infrastructure asset or major reconstruction project, the bidding and procurement process requires the development and inclusion of a DBT, and subsequent development of security performance specifications.[93]

2. Benefits

Unlike the relatively simple approach that can be taken for government buildings, applying safety and security to other infrastructure types can vary greatly. To influence change over this vast range of asset types can be very challenging that requires an even more flexible and adaptive approach. Unlike the aforementioned first recommendation provided, many of the projects that would be included in this category are not under the OGS's control, which provides the DHSES the opportunity to take the lead and champion the concept of incorporating safety and security components through planning and design. By requiring an early partnership with the infrastructure owner/operator and the DHSES prior to the planning and design phase for state financed infrastructure projects, the state can ensure that the safety and security discussion is incorporated early in the process and is communicated as a requirement. Leveraging skills sets resident within the DHSES and existing expertise within the owner/operator group, the assigned team can focus the planning and design process on relevant threats, and require communication concerning how their proposed design would withstand the identified threats. This process would be utilized to assist the determination of a final contract award.

[93] Department of Defense, Defense Standardization Program, "Frequently Asked Questions about Performance Specifications," n.d., http://www.dsp.dla.mil/APP_UIL/displayPage.aspx?action=content&accounttype=displayHTML&contentid=28.

3. Challenges

NYS provides funds connected to infrastructure in one form or another through multiple avenues. It is possible that the universe, which this recommendation would affect, will be larger than the chosen DBT development team could handle. To mitigate this issue, a minimum project monetary threshold may need to be considered to ensure the scale and scope is one that NYS can manage effectively.

This process also requires effective collaboration between the infrastructure owner/operator and the assigned DHSES team. Included within the DBT, the DHSES will share a detailed threat assessment, which will provide information, such as historically related incidents, attack methods, and recent trends. This product will then need to be leveraged in collaboration with all stakeholders to apply the completed threat assessment to the actual infrastructure to complete the DBT. To ensure sensitive information is protected from release to unauthorized personnel, a project specific non-disclosure process will be leveraged. Once complete, the owner/operator team will be ultimately responsible for publishing the final DBT and security performance specification. If the owners/operators either do not buy into the process or do not agree with the discussed threats, the final version provided to bidders may lead to responses that do not significantly address safety and security.

Finally, the current staffing available within the DHSES to accomplish this work would create several concerns. Like many agencies, the personnel who would be assigned to accomplish this work within the DHSES already have assigned tasks and responsibilities. Leadership would have to either make a decision to reprioritize efforts, discontinue programs and/or hire new personnel. Additionally, the flexibility allowed in this approach may vary the type of infrastructure projects that the DHSES is involved with greatly. Projects could swing dramatically from transportation structures to water and wastewater facilities. This variance could challenge the expertise available with the DHSES to create informed DBT products that truly contribute to the process. It is extremely unlikely that the DHSES would be able to hire subject matter experts for every sector; therefore, a more creative and flexible approach to mitigating this issue will have to be established—perhaps utilizing contractors, part-time personnel, or employees

temporarily detailed for a specific timeframe to supplement existing expertise. Developing an uninformed DBT could potentially do more harm than good as resources would end up being spent in unneeded areas.

4. Next Steps

As an initial step, DHSES leadership should meet with the Department of Budget (DOB) to discover the scale and scope of NYS fund distribution to new and major reconstruction projects to inform the process and assist with understanding whether a minimum project monetary threshold should be included in the proposal. To ensure the team does not take on more than it can handle, it is recommended that the threshold err of the side of a higher monetary threshold than a lower one. Once completed, the concern of taking on more than the existing team can handle will be mitigated.

Second, the DHSES should meet with those responsible for managing the "Rebuild NY" State Infrastructure Bank[94] to discuss the concept of requiring funded projects to include a DBT product and security performance specifications. If this process is initiated prior to funds being awarded, it should limit the ability for owner/operator groups to resist or challenge its inclusion. It would be suggested that a pilot period be utilized to test the concept and allow for evaluation prior to full implementation. This test period will allow the DHSES to gauge how effectively the assigned team and owner/operators collaborate together. Since a regulatory/mandatory incentive is not being utilized, it will be very important to measure success qualitatively for the pilot period. If collaboration does not work well during this period, a more stringent approach may need to be developed, and a reevaluation will be necessary.

Third, once the concept has been agreed upon, a DBT team will need to be developed internally within the DHSES, and the OCT would be the most appropriate office to be assigned this duty. Leveraging individuals from the Critical Infrastructure Protection Unit and the Intelligence and Analysis Unit, a core group could be formed to focus on this task. To accomplish this task with the least impact to current operations, additional personnel would be required to be hired by the office. For the initial pilot

[94] New York State, "NY Works."

period, the addition of one full time equivalent to both the Critical Infrastructure Protection Unit and the Intelligence and Analysis Unit would provide the staffing needs.

Fourth, to address the concerns regarding a lack of subject matter expertise, two realistic options are available. First, leveraging the DHSES's state role in which both federal and local assets are relatively accessed with ease, the group could focus on building networks, which could be utilized for information when necessary. Additionally, NYS has a multitude of agencies, which could be leveraged when working on a particular infrastructure type. One example would be a hospital project; the DBT team could work closely with the NYS Department of Health to obtain the subject matter expertise it may be lacking. Another option would be to develop a pool of part-time personnel who could be brought on for specific projects. An example of this type of pool exists within the NYS Office of Emergency Management, Public Assistance Liaison Program,[95] which was created in 1998. Now working under a new title of Disaster Assistance Representatives, these individuals are interviewed and evaluated for particular subject matter expertise and then kept in an inactive status until their skill set is needed. When an incident occurs that requires their expertise, they are offered the opportunity to be brought on for a period of time.

Prior to, and during, the pilot phase, the available group should be tasked with reviewing existing DBT models (such as the one utilized by the IAEA) and developing a rational standard process. This process would work the group through each required step of developing a DBT. Additionally, it would provide options for obtaining the necessary subject matter expertise.

Finally, once all those steps have been completed, the program could move to the execution phase, in which the partnership between the DHSES and the owner/operator stakeholders can be tested and evaluated. Developed DBTs would be incorporated with owner/operator knowledge to design performance specifications, which would be included in the request for proposals. Final products included within the bidding process will demonstrate if the goals of incorporating an informed safety and security process are

[95] New York State, Division of Homeland Security and Emergency Services, "Public Assistance Liaison Program," n.d., http://www.dhses.ny.gov/oem/recovery/pal-program.cfm.

being met. The pilot period will also allow time to review responses from bidders and develop an understanding as to whether bidders are responding in a favorable manner to the performance specifications.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSION

Protecting NYS's infrastructure is a responsibility that many different stakeholders are charged with both in the public and private sectors. As responsible government employees, those charged with protecting the state's infrastructure should ensure the programs and works being completed are done so effectively and efficiently.

Two research questions were asked in this thesis.

- What are the benefits and challenges of NYS placing a greater focus on the planning, engineering and design phase for new or majorly reconstructed infrastructure?
- How could a new partnership model at the state level be designed to support infrastructure protection activities during this phase?

Prior to answering these questions, an intensive literature review was conducted to explore efforts in this field within both the public and private realm. A structured and focused analysis was then completed on several approaches of groups that demonstrated action in this field. During this analysis, it became evident that the participation incentive utilized to accomplish the identified goals was a core component for success in developing a new program. Understanding this component, additional analysis was completed on the identified varieties of participation incentives.

Through research on infrastructure challenges facing NYS and the United States, several issues (reacting to an event, risk issues, etc.) were identified and demonstrate the complexity of this issue. Recognizing that, once built, infrastructure exists and is utilized for long timeframes, and later cycle adjustments and security improvements are very expensive, it is critical that these assets are initially constructed to the highest quality in all regards.

Overall, this change in focus for NYS into the planning, engineering, and design environment will greatly assist the state's infrastructure for the long term. Starting this process by first improving state owned buildings would demonstrate to the community that NYS takes this subject matter seriously. This process will also allow the DHSES the opportunity to continue to improve its expertise in enhancing safety and security through

planning, engineering, and design. Additionally, requiring security to be a focus for assets that receive state funds will demonstrate to contractors and the community the same priorities. Leveraging the DBT process to guide the development of performance specification with owner/operators will ensure this new process is appropriately focused.

To be successful, NYS must also recognize its limitations. Many different approaches and participation models can be leveraged, stretching resources too thin by attempting too many could be counterproductive. Multiple challenges exist that should be evaluated in depth and clearly understood, as seen in the Appendix. Lessons learned from recent regulatory programs, such as CFATS, teach government to be pragmatic with an identified approach and not to stretch resources too thin. CFATS demonstrated that understaffing a program can lead to frustrations at both the owners/operators and legislative levels. Staffing concerns are a real issue for the DHSES as these recommendations are explored and cannot be taken lightly.

Although focused effort will be placed on mandatory participation models, this does not discourage the use of other voluntary and fiscally incentivized tools, particularly for the broader world of privately owned and funded infrastructure. It may be challenging to evaluate the effectiveness of these approaches; however, at the very least, they support the safety and security narrative. Hopefully, the aggregate of all these approaches by stakeholders supports the overall goal of creating a resilient state.

Finally, more research should be done to ascertain the effectiveness of programs being implemented in this field. Surveying the owners/operators of the infrastructure on which these programs are focused could potentially provide detailed insight into their value. Findings from surveys targeted on the varying types of partnership incentive tools would produce currently non-existent important data that could be analyzed.

APPENDIX

Challenges To Implenting Safety and Security Measures Through Planning, Engineering and Design		
	State-Owned	**State-Financed**
Fiscal Concerns	**Yes**: Although incorporating improved security measures during planning and design is less costly than doing so once an asset has been built, it remains an expense. Any increased expenses for state owned assets will likely be challenging for agency budgets and plans.	**Yes:** By requiring security measures to be incorporated within the bidding process it will ultimately affect the bottom line of bidder proposals.
Relinquishment of Authority	**Yes**: With the inclusion and implementation of security measures delegated to the individual agency there may be hesitancy by individual leadership groups to relinquish that authority. Leadership may view this as a less beneficial process than their previously developed internal policies.	**No:** This process will be executed on a contract by contract basis and will face the authority challenges recognized by state-owned buildings. To receive state finacing for the infrastructure project it will simply be a requirement built into the agreement.
Perceived Lack of Threat	**Yes**: Affected leadership may argue that the overall risk to the group does not justify the need to develop and implement standards.	**Yes:** The collaboration portion of this process requires an effective partnership between the developer of the DBT and the owner/operator. If the owner/operator does not support the threat findings the final product may be impacted negatively.
Complicated Process	**No**: Representing a simple government approach once the mandate and standards have been issued there should be a clear and uncomplicated path to follow.	**Yes:** Unlike the mandated process, this will require a flexible approach which must be tailored to the infrastructure type for each new project. It will require involvment of subject matter expertise and sound teamwork.
Staffing Constraints	**Yes:** Although staffing issues can be mitigated by reivigorating existing units and partnerships the efforts required to create standards and manage the process will require previously unplanned for staff hours.	**Yes**: This will require hiring additional staff to fill these roles and periodically leveraging other available subject matter experts.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adams, Walter "Skip," and Deborah A. Somers. "Codes, Standards, and Guidelines for Security Planning and Design." In *Building Security: Handbook for Architectural Planning and Design*, edited by Barbara Nadel. New York, NY: McGraw-Hill, 2004.

Alexander, George, and Bennet Andrew. *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, 2005.

American Institute of Architects, The. *Statement of Barbara A. Nadel, Too Much for Too Little: Finding the Cost-Risk Balance for Protecting Federal Employees in Leased Facilities, House Subcommittee on Economic Development, Public Buildings and Emergency Management*, May 20, 2010.

American Society of Civil Engineers. "Report Card for America's Infrastructure." (n.d.). http://www.infrastructurereportcard.org/.

ASCE Critical Infrastructure Guidance Task Committee. *Guiding Principles for the Nation's Critical Infrastructure*. Reston, VA: American Society of Civil Engineers, 2009.

ASIS International. "American Society for Industrial Security." (n.d.). https://www.asisonline.org/Pages/default.aspx.

Bardach, Eugene. "Part Three: "Smart (Best) Practices"—Research: Understanding and Making Use of What Look Like Good Ideas from Somewhere Else." In *Practical Guide for Policy Analysis, The Eightfold Path to More Effective Problem Solving*. 4th ed. Berkeley, CA: University of California, 2012.

Barros, Pedro Pita, and Xavier Martinez-Giralt. "Contractual Design and PPPs for Hospitals: Lessons for the Portuguese Model." *The European Journal of Health Economics* 10, no. 4 (October 2009), 437–453.

Becker, Fred, and Valerie Patterson. "Public: Private Partnerships: Balancing Financial Returns, Risks, and Roles of the Partners." *Public Performance & Management Review* 29, no. 2 (December 2005), 125–144.

Cabinet Office. "National Risk Register." 2008. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61929/CO_NationalRiskRegister_2012_acc.pdf.

Cameron, David et al. “A Strong Britain in an Age of Uncertainty: The National Security Strategy.” *Stationery Office*, October 2010. http://www.cabinetoffice.gov.uk/sites/default/files/resources/national-security-strategy.pdf.

Centre for the Protection of National Infrastructure. *Integrated Security: A Public Realm Design Guide for Hostile Vehicle Mitigation*, 2011.

———. *Protecting Against Terrorism: 3rd Edition*, 2010.

Centre for the Protection of National Infrastructure and British Transport Police. *Security in the Design of Stations Guide*, 2012.

Commission for Architecture and the Built Environment. “London 2012 Reviews.” (n.d.). http://webarchive.nationalarchives.gov.uk/20110118095356/http://www.cabe.org.uk/design-review/london-2012.

Demkin Joseph A., and American Institute of Architects. *Security Planning and Design : A Guide for Architects and Building Design Professionals*. Hoboken, NJ: J. Wiley & Sons, 2004.

Department of Defense. Defense Standardization Program. “Frequently Asked Questions about Performance Specifications.” (n.d.). http://www.dsp.dla.mil/APP_UIL/displayPage.aspx?action=content&accounttype=displayHTML&contentid=28.

Department of Homeland Security. “DHS Risk Lexicon.” September 2008. http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf.

———. “Interagency Security Committee Standards and Best Practices.” (n.d.). https://www.dhs.gov/interagency-security-committee-standards-and-best-practices.

Design-Build Institute of America. “About.” (n.d.). http://www.dbia.org/Pages/default.aspx.

Division of Homeland Security and Emergency Services. “Critical Infrastructure Protection Unit.” (n.d.). http://www.dhses.ny.gov/oct/units/critical-infrastructure-protection/.

Eckert, Sue. *Protecting Critical Infrastructure: The Role of the Private Sector*. Ridgway Center Working Papers, 2005.

Estes, Adam. “The Exploding Fertilizer Plant in Texas Hadn’t Had a Full Inspection in Three Decades.” *The Atlantic Wire*, 2013.

Federal Emergency Management Agency. “Authorized Equipment List.” (n.d.). https://www.rkb.us/mel.cfm?subtypeid=549.

———. “FY 2013 Homeland Security Grant Program.” (n.d.). http://www.fema.gov/fy-2013-homeland-security-grant-program-hsgp-0.

———. *Hazard Mitigation Assistance Unified Guidance*, 2013.

Gallaher, Michael P., and Robert E. Chapman. *Cost Analysis of Inadequate Interoperability in the U.S. Capital Facilities Industry*. Gaithersburg, MD: U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology 2004.

General Services Administration. “Design and Construction Overview.” (n.d.). http://www.gsa.gov/portal/content/104549?utm_source=PBS&utm_medium=print-radio&utm_term=HDR_1_Bldgs_design&utm_campaign=shortcuts.

———. *Design Excellence: Policies and Procedures*, 2004.

———. “Guiding Principles for Federal Architecture.” (n.d.). http://www.gsa.gov/portal/content/136543.

Gibbs, Linda, and Caswell Holloway. *Hurricane Sandy After Action: Report and Recommendations to Major Michael R. Bloomberg*, New York City, NY, 2013.

Glancey, Jonathan. “Constructive Criticism: The Week in Architecture.” *The Guardian*, 2011.

GoodReads. “Never Let a Good Crisis Go to Waste.” (n.d.). http://www.goodreads.com/quotes/717228-never-let-a-good-crisis-go-to-waste.

Governor’s Press Office. *Governor Cuomo Announces Commissions to Improve New York State’s Emergency Preparedness and Response Capabilities, and Strengthen the State’s Infrastructure to Withstand Natural Disasters*. New York State, November 28, 2012.

Hardin, Garrett James, and American Association for the Advancement of Science. *The Tragedy of the Commons*. Washington, DC: American Association for the Advancement of Science, 1968.

Home Office Design and Technology, Alliance Against Crime and the Design Council. *Design Out Crime: Case Studies, Examples of Design Being Used to Tackle Crime Problems Around the World*, 2011.

International Atomic Energy Agency. “Implementing Guide, Development, Use and Maintenance of the Design Basis Threat.” IAEA Nuclear Security Series no. 10, 2009. http://www-pub.iaea.org/MTCD/publications/PDF/Pub1386_web.pdf.

Kirkham, Lara, with Alan J. Kuperman. “Protecting U.S. Nuclear Facilities from Terrorist Attack: Re-Assessing the Current “Design Basis Threat” Approach.” *The University of Texas Blog Service*, August 15, 2013. blogs.utexas.edu/nppp/files/2013/08/NPPP-working-paper-1-2013-Aug-15.pdf.

Leach, Terry. “Federally Owned or Leased Office Buildings: Security Design.” In *Building Security: Handbook for Architectural Planning and Design*, edited by Barbara Nadel. New York, NY: McGraw-Hill, 2004.

Ljeh, Ike. “Euston, We Have a Problem.” *Building.Co.Uk*, June 21, 2013. http://www.building.co.uk/euston-we-have-a-problem/5056620.article.

McCarthy, Kevin E. et al. *Recommendations on Improving Infrastructure Resilience Post-Sandy*. Hartford, CT: Connecticut General Assembly, Office of Legislative Research, 2013.

McConnell, John. *Re: Notice of Inquiry—Incentives to Adopt Improved Cybersecurity Practices*. (Docket Number 130206155-3155-01). Booze Allen Hamilton, 2013.

Metropolitan Transit Authority. “Remembering and Rebuilding After 9/11.” September 10, 2010. http://new.mta.info/news/2010/09/10/remembering-and-rebuilding-after-9-11.

———. “Restoring South Ferry Station.” (n.d.). http://web.mta.info/nyct/service/RestoringSouthFerryStation.htm.

Nadel, Barbara A. *Building Security: Handbook for Architectural Planning and Design*. New York, NY: McGraw-Hill, 2004.

National Institute of Building Sciences. “Whole Building Design Guide.” (n.d.). http://www.wbdg.org/.

New York City Police Department. *Engineering Security: Protective Design for High Risk Buildings*, 2009.

New York State. “NY Works.” (n.d.). http://andrewcuomo.com/nyworks.

———. Division of Homeland Security and Emergency Services. “Public Assistance Liaison Program.” (n.d.). http://www.dhses.ny.gov/oem/recovery/pal-program.cfm.

New York State Office of Emergency Management. “Hazard Mitigation Grant Program.” (n.d.). http://stormrecovery.ny.gov/content/hazard-mitigation-grant-program-hmgp-0.

NYS Department of Transportation. “Kosciuszko Bridge Project.” (n.d.). https://www.dot.ny.gov/kbridge.

Office of General Services. “Security and Emergency Management Unit.” (n.d.). http://ogs.ny.gov/BU/BA/SEMU.asp.

Reed Construction Data/RSMeans Market Intelligence. *Design-Build Project Delivery Market Share and Market Size Report*, 2013.

“Research and Markets: Handbook of Loss Prevention and Crime Prevention. Edition No. 5.” *Journal of Engineering* (September 26, 2012): 1245.

Spadanuta, Laura. “The Greening of Security.” *Security Management*, n.d.

U.S. Department of Homeland Security, Science and Technology Directorate. “DHS Building and Infrastructure Protection Series Tools.” (n.d.). http://www.dhs.gov/building-and-infrastructure-protection-series-tools-0.

U.S. Green Building Council. “Leadership in Energy & Environmental Design.” (n.d.). http://www.usgbc.org/leed.

U.S. House of Representatives Chairman Fred Upton. *Congressional Leaders Express Reservations about Extending CFATS Funding in Light of Program’s Failures*, Energy & Commerce Committee, 2013.

United States and the Department of Homeland Security. *National Infrastructure Protection Plan*. Washington, DC: U.S. Department of Homeland Security, 2006.

———. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington, DC: Department of Homeland Security, for sale by the Supt. of Docs, U.S. GPO, 2003.

Van Ekeren, Glenn. *Words for all Occasions*. Rowe, MA: Prentice Hall, 1988.

WBDG Aesthetics Subcommittee. National Institute of Building Sciences. “Engage the Integrated Design Process.” Last updated November 5, 2012. http://www.wbdg.org/design/engage_process.php.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California